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: Proposed rule; request for public comment.

SUMMARY: The Consumer Financial Protection Bureau (CFPB) is proposing a rule to implement personal financial data rights under the Consumer Financial Protection Act of 2010 (CFPA). The proposed rule would require depository and nondepository entities to make available to consumers and authorized third parties certain data relating to consumers' transactions and accounts; establish obligations for third parties accessing a consumer's data, including important privacy protections for that data; provide basic standards for data access; and promote fair, open, and inclusive industry standards.

DATES: Comments must be received on or before December 29, 2023.

ADDRESSES: You may submit comments, identified by Docket No. CFPB–2023–0052 or RIN 3170–AA78, by any of the following methods:

- *Federal eRulemaking Portal: https://www.regulations.gov.* Follow the instructions for submitting comments. A brief summary of this document will be available at *https://www.regulations.gov/docket/CFPB-2023-0052.*
- *Email: 2023-NPRM-Data-Rights@cfpb.gov.* Include Docket No. CFPB–2023–0052 or RIN 3170–AA78 in the subject line of the message.
- *Mail/Hand Delivery/Courier:* Comment Intake—FINANCIAL DATA RIGHTS, c/o Legal Division Docket Manager, Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

Instructions: The CFPB encourages the early submission of comments. All submissions should include the agency name and docket number or Regulatory Information Number (RIN) for this rulemaking. Commenters are encouraged to submit comments electronically. In general, all comments received will be posted without change to *https://www.regulations.gov.*

All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Proprietary information or sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Submissions will not be edited to remove any identifying or contact information.

FOR FURTHER INFORMATION CONTACT: Dave Gettler, Paralegal Specialist; Anna Boadwee or Vince Mancini, Attorney-Advisors; Briana McLeod, Counsel; Joseph Baressi, Sarita Frattaroli, David Jacobs, Mark Morelli, Kristen Phinnessee, Michael Scherzer, Yaritza Velez or Priscilla Walton-Fein, Senior Counsels, 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

The following abbreviations and acronyms are used in this proposed rule:

ACH = Automated Clearing House
ANPR = Advance Notice of Proposed Rulemaking
API = Application programming interface
APR = Annual percent rate
ATO = Account takeover
BLS = Bureau of Labor Statistics
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 = 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
OMB = Office of Management and Budget
SBA = Small Business Administration
SSN = Social Security number
TAN = Tokenized account number
URL = Uniform resource locator

I. Background

A. Introduction

Digitization and decentralization in consumer finance create new possibilities for more seamless consumer switching and greater competitive intensity. For example, when consumers are able to share their personal financial data, they can share details about their income and expenses that may give lenders more confidence when extending credit. When a consumer can switch with less friction, this will create incentives for superior customer service and more favorable terms. At the same time, sharing personal financial data can also lead to misuse and abuse, given its commercial value.

In 2010, Congress explicitly recognized the importance of personal financial data rights in section 1033 of the Consumer Financial Protection Act of 2010 (CFPA).[1] However, to date, the CFPB has not issued a rule to implement this provision of law.

Many market participants have already sought to develop technologies and standards to facilitate consumer access to personal financial data. The CFPB intends to accelerate the shift to a more open and decentralized system through the issuance of a final rule.

[1] The CFPA is title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111–203, 124 Stat. 1376, 2008 (2010).

B. Electronic Access to Personal Financial Data

Development of Electronic Data Access

By 1999, 20 percent of national banks offered online banking, including all national banks with over $10 billion in assets, and accounting for over 80 percent of all small deposit accounts held by national banks.[2] Adoption grew from 14 million consumers in 2000 to 37 million in 2002, and to 53 million in 2004.[3] Around this time, the first wave of online-only financial services providers emerged. In the late 2000s, smartphones made digital banking still more available.

Today, 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.

Development of Open Banking

Building on these developments, open banking [5] 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.[6] These developer interfaces facilitated consumer-authorized data access that was necessary for many new products and services. Third parties often outsourced establishing and maintaining connections with data providers to data aggregators. These intermediaries largely relied on ''screen scraping,'' which uses consumer credentials to log in to consumer accounts to retrieve data.[7] Widespread screen scraping allowed open banking to grow quickly in the United States.

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. Aggregators often declined to seek permission from financial institutions they ''scraped,'' and some methods aggregators used to solicit credential sharing led to litigation.[8] In late 2015, several large retail banks took actions that disrupted screen scraping, albeit temporarily.[9]

Around that same time, efforts accelerated to establish agreements for third parties to access data via a provider's developer interface.[10] While the progress of access agreements has been uneven, the open banking system has nevertheless grown as consumer reliance on products and services powered by consumer-authorized data access expanded. This growth led to further disputes and litigation between system participants,[11] and concerns over privacy and harmful uses of consumer-authorized data increased.[12]

Despite these challenges, financial institutions have begun to dedicate more resources to develop open banking infrastructure. This includes multilateral efforts, some of which have been controversial.[13] Other incumbents, most notably large payment networks, have sought to acquire aggregators.[14]

---

[2] Alyssa Bentz, *First in Online Banking,* Wells Fargo Corp. Archives (Mar. 14, 2019), *https://www.wellsfargohistory.com/first-in-online-banking/*; Karen Furst *et al., internet Banking: Developments and Prospects,* Off. of the Comptroller of the Currency (2000), *https://www.occ.treas.gov/publications-and-resources/publications/economics/working-papers-archived/pub-econ-working-paper-2000-9.pdf.*

[3] Susannah Fox, *Online Banking 2002,* Pew Rsch. Ctr. (Nov. 17, 2002), *https://www.pewresearch.org/internet/2002/11/17/online-banking-2002/;* Susannah Fox, *Online Banking 2005,* Pew Rsch. Ctr. (Feb. 9, 2005), *https://www.pewresearch.org/internet/2005/02/09/online-banking-2005/.*

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

[5] This **Federal Register** notice 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 United States.

[6] 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/.*

[7] Unless otherwise stated, the term ''screen scraping'' in this document refers to credential-based screen scraping, which is prevalent in the market today.

[8] *See, e.g.,* Plaid, Inc., *In re Plaid, Inc. Privacy Litigation—Frequently Asked Questions, https://www.plaidsettlement.com/frequently-asked-questions.php* (last visited Sept. 18, 2023); TD Bank, *TD Bank Files Trademark Counterfeiting and Infringement Lawsuit Against Plaid in the U.S.* (Oct. 14, 2020), *https://stories.td.com/us/en/article/td-bank-files-trademark-counterfeiting-and-infringement-lawsuit-against-plaid-in-the-u-s;* Penny Crosman, *PNC sues Plaid for trademark infringement,* Am. Banker (Dec. 23, 2020), *https://www.americanbanker.com/news/pnc-sues-plaid-for-trademark-infringement.*

[9] Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals,* Wall St. J. (Nov. 4, 2015), *https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450;* Peter Rudegeair, *J.P. Morgan Warns It Could Unplug Quicken and Quickbooks Users,* Wall St. J. (Nov. 24, 2015), *https://www.wsj.com/articles/j-p-morgan-may-unplug-some-customers-access-to-account-data-1448375950;* Daniel Huang & Peter Rudegeair, *Bank of America Cut Off Finance Sites From Its Data,* Wall St. J. (Nov. 9, 2015), *https://www.wsj.com/articles/bank-of-america-cut-off-finance-sites-from-its-data-1447115089.*

[10] *See, e.g.,* Penny Crosman, *Wells Fargo strikes data-sharing agreement with Plaid,* Am. Banker (Sept. 19, 2019), *https://www.americanbanker.com/news/wells-fargo-strikes-data-sharing-agreement-with-plaid;* Finicity, *Enhancing the Data-sharing Experience at USAA* (July 2, 2018), *https://www.finicity.com/blog/data-sharing-usaa-direct-api/;* Mary Wisniewski, *JPMorgan Chase and Finicity ink data-sharing agreement,* Am. Banker (July 11, 2017), *https://www.americanbanker.com/news/jpmorgan-chase-and-finicity-ink-data-sharing-agreement.*

[11] Nathan DiCamillo, *In data dispute with Capital One, Plaid stands alone,* Am. Banker (July 17, 2018), *https://www.americanbanker.com/news/in-data-dispute-with-capital-one-plaid-stands-alone;* Yuka Hayashi, *Venmo Glitch Opens Window on War Between Banks, Fintech Firms,* Wall St. J. (Dec. 14, 2019), *https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402;* Penny Crosman, *PNC sues Plaid for trademark infringement,* Am. Banker (Dec. 23, 2020), *https://www.americanbanker.com/news/pnc-sues-plaid-for-trademark-infringement;* TD Bank, *TD Bank Files Trademark Counterfeiting and Infringement Lawsuit Against Plaid in the U.S.* (Oct. 14, 2020), *https://stories.td.com/us/en/article/td-bank-files-trademark-counterfeiting-and-infringement-lawsuit-against-plaid-in-the-u-s.*

[12] *See, e.g.,* Maeve Allsup, *App Users Say Plaid Collects Bank Logins Without Consent,* Bloomberg L. (May 5, 2020), *https://news.bloomberglaw.com/class-action/app-users-say-plaid-collects-bank-logins-without-consent;* Ron Wyden, *Wyden, Brown, Eshoo Urge FTC to Investigate Firm Collecting and Selling Americans' Financial Data* (Jan. 17, 2020), *https://www.wyden.senate.gov/news/press-releases/wyden-brown-eshoo-urge-ftc-to-investigate-firm-collecting-and-selling-americans-financial-data.*

[13] *E.g.,* OpenID Found., *Announcing the Financial API (FAPI) Working Group* (May 23, 2016), *https://openid.net/announcing-the-financial-api-fapi-working-group/;* Fin. Data Exch., *Financial Industry Unites to Enhance Data Security, Innovation and Consumer Control* (Oct. 18, 2018), *https://www.financialdataexchange.org/FDX/FDX/News/Press-Releases/Financial_Industry_Unites_Data_Security.aspx; E.g.,* Penny Crosman, *Fidelity data-sharing hub aims to end screen scraping,* Am. Banker (June 11, 2019), *https://www.americanbanker.com/news/fidelity-data-sharing-hub-aims-to-end-screen-scraping;* PR Newswire, *S&P Global enhances KY3P® risk management capabilities with acquisition of TruSight Solutions LLC* (Jan. 9, 2023), *https://www.prnewswire.com/news-releases/sp-global-enhances-ky3p-risk-management-capabilities-with-acquisition-of-trusight-solutions-llc-301715878.html;* Penny Crosman, *Fidelity's data-sharing unit Akoya to be jointly owned with The Clearing House, 11 banks*(Feb. 20, 2020), *Am. Banker, https://www.americanbanker.com/news/fidelitys-data-sharing-unit-akoya-to-be-jointly-owned-with-the-clearing-house-11-banks.*

[14] *See, e.g.,* Visa, *Visa to Acquire Plaid* (Jan. 13, 2020), *https://usa.visa.com/about-visa/newsroom/*

Continued

Most recently, large payments-focused nondepositories have looked to enter the aggregation space by developing internal business units, sometimes partnering with incumbent aggregators.[15] These efforts indicate the potential for incumbents to mitigate or neutralize competitive threats from open banking, demonstrating the need for strong rules to protect the openness of the system.

State of the Open Banking System

The CFPB estimates that at least 100 million consumers have 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 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.[16]

The open banking system also engages a large number of entities. While loans and deposits in the United States are concentrated among the largest depositories, there are more than nine thousand banks and credit unions across the country,[17] most of which serve as data providers, as do numerous nondepository financial institutions.[18] The number of third parties may total as many as ten thousand, driven by a large financial technology sector.[19] A growing number of entities now serve as both data providers and third parties. For example, many depositories now offer personal financial management tools, while some so-called neobank accounts and digital wallets serve as important transaction accounts for consumers. Most third party access is effectuated via a small number of aggregators, although some third parties elect to access at least some data directly.

Third party data access is generally enabled by one of two methods. In screen scraping, consumers usually share their consumer interface credentials with a third party or their service provider. That entity uses (and may store) those credentials to access the consumer's account to retrieve data for use in the third party's products and services. The second method is through developer interfaces maintained by data providers or their service providers. These often take the form of APIs that can be accessed without consumer credentials, for example, by using secure tokens. Such interfaces enable the direct transmission of structured machine-readable data, promote standardization, and reduce risks of inaccuracies and security breaches, among other benefits. Data providers also have offered APIs accessed using consumer interface credentials or deployed tokenized access to their consumer interface, but most stakeholders agree that such measures are best viewed as a stopgap, and that credential-free access to developer interfaces is preferable.

Based on feedback received through public comments and stakeholder outreach, there is nearly universal consensus that developer interfaces should supplant screen scraping.[20] Stakeholders responding to the SBREFA Outline, including small entity representatives, several data aggregators, data providers, and a trade association representing third party data recipients and aggregators, supported a general transition towards the use of developer interfaces.[21] However, such a transition requires certain conditions. First, data providers must commit resources to develop and maintain developer interfaces. While large depository and nondepository institutions might have sufficient information technology budgets to do this themselves, small institutions tend to rely on a few core service providers, and frequently report problems with the services that ''cores'' offer. Second, connecting to a developer interface generally requires a third party to agree to a data provider's terms of access, a process that has been impeded as discussed below. Today, the CFPB estimates that about half of third party data access currently occurs through APIs; scraping comprises the bulk of the balance. This is a significant shift: as recently as 2021, most access was via screen scraping. Much of this progress has been concentrated among the largest data providers.

Open banking use cases continue to emerge and develop. Major use cases, which the CFPB understands generally rely heavily or exclusively on data from transaction accounts, include personal financial management tools of all kinds, 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. Many use cases also compete with the core offerings of other types of financial institutions, such as card networks and credit bureaus.[22]

C. Challenges in the Open Banking System

Despite these developments, commercial actors are able to use their market power and incumbency to privilege their concerns and interests above fair competition that could benefit consumers. 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 negotiation of access agreements and the development of market-wide standards. This leads to inconsistent data access for consumers

press-releases.releaseId.16856.html; Visa, *Visa Completes Acquisition of Tink* (Mar. 10, 2022), *https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.18881.html;* Mastercard, *Mastercard to Acquire Finicity to Advance Open Banking Strategy* (June 23, 2020), *https://www.finicity.com/in-the-news/mastercard-to-acquire-finicity-to-advance-open-banking-strategy/.*

[15] *See, e.g.,* John Adams, *Stripe adds tech for Plaid-like account aggregation,* Am. Banker (May 4, 2022), *https://www.americanbanker.com/payments/news/stripe-adds-tech-for-plaid-like-account-aggregation;* Klarna, *Klarna launches 'Klarna Kosma' sub-brand and business unit to harness rapid growth of Open Banking platform* (Mar. 31, 2022), *https://www.klarna.com/international/press/klarna-launches-klarna-kosma-sub-brand-and-business-unit-to-harness-rapid-growth-of-open-banking-platform/.*

[16] *See* Competition & Mkts. Auth., *UK reaches 7 million Open Banking users milestone* (Feb. 20, 2023), *https://www.openbanking.org.uk/news/uk-reaches-7-million-open-banking-users-milestone/,* and Bnamericas, *Open Finance completes two years with 17.3 million customer consents* (Feb. 2, 2023), *https://www.bnamericas.com/en/news/brazil-open-finance-completes-two-years-with-173-million-customer-consents.*

[17] Fed. Deposit Ins. Corp., *Statistics at a Glance—Industry Trends* (Mar. 31, 2023), *https://www.fdic.gov/analysis/quarterly-banking-profile/statistics-at-a-glance/2023mar/industry.pdf;* Nat'l Credit Union Admin., *Quarterly Credit Union Data Summary—2022 Q4* (Mar. 8, 2023), *https://ncua.gov/files/publications/analysis/quarterly-data-summary-2022-Q4.pdf.*

[18] Some aggregators report even more data providers. *See, e.g., https://plaid.com/* (over 12,000 as of Sept. 16, 2023); *https://www.mx.com/*(over 13,000 as of Sept. 16, 2023); *https://docs.finicity.com/search-institutions/*(over 16,000 as of Sept. 16, 2023); *https://www.yodlee.com/data-aggregation* (over 17,000 as of Sept. 16, 2023).

[19] In 2022, Plaid indicated that they alone have over 6,000 customers. Plaid, *Ushering in Fintech's Next Phase* (May 19, 2022), *https://plaid.com/blog/ushering-in-fintechs-next-phase/.*

[20] *See, e.g.,* Consumer Fin. Prot. Bureau, *Bureau Symposium: Consumer Access to Financial Records Report,* at 3–4 (July 2020), *https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.*

[21] *See* Consumer Fin. Prot. Bureau, *Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration of the Required Rulemaking on Personal Financial Data Rights,* at 30–31 (Mar. 30, 2023), *https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf.*

[22] Conversely, data-sharing schemes owned by large depositories can also compete with open banking-supported products and services; *see, e.g.,* Early Warning Sys., *Verify Identity—Expand your customer base with confidence, https://www.earlywarning.com/products/verify-identity* (last visited Sept. 7, 2023).

and costs for the market. Most notably, these dynamics impel third parties to rely on intermediaries. The commercial interests of such intermediaries may not always advance open banking, since they stand to benefit from protecting private network effects against open standards that could displace them or lower their rents.

Market participants' interests may diverge due to interrelated competitive, legal, and regulatory factors. Data providers may minimize the data they share or refrain from sharing altogether to protect their market position. Data providers may also have data security, risk management, and data privacy concerns regarding consumer-authorized access to their data and systems.[23] Motivated by their own self-interest, third parties may use screen scraping to collect more data than they reasonably need. Diverging self-interests also lead to disagreements over issues such as the frequency and duration of data access, the imposition of access caps, the assignment of liability, and consumer authorization procedures. These dynamics undermine the efficient functioning of the open banking system for consumers and the system's ability to move away from screen scraping.

Third parties' data use can also contribute to problems in the current open banking system. When consumers go into the market to obtain a product, they do not want third parties to serve their own commercial interests by collecting, using, or retaining data beyond what they need to provide that product.[24] For example, third parties with surveillance revenue models monetize consumer data by targeting consumers with unwanted ads or services or selling the consumer data, undermining consumers' ability to limit data use to providing the product they sought. Third parties also collect data using methods that may compromise consumers' data privacy, security, and accuracy, as well as data provider interests related to security, liability, and risk management. For example, screen scraping may pose risks to consumers' data privacy and security by capturing and storing consumer credentials and potentially capturing more data than are reasonably necessary to provide the requested product or service. Additionally, because screen scraping requires a third party to parse through a data provider's consumer interface and transpose the unstructured information that a consumer sees into a structured format the third party can use, any errors in the transposition or any changes a data provider makes to the consumer interface can increase the risks of data inaccuracy in the third party's product or service. Screen scraping also presents risks to data providers because it involves third parties accessing data on an automated basis from a system not designed for that purpose, leading some data providers to report that screen scraping puts undue strain on their information systems. Screen scraping exacerbates data provider concerns with respect to liability, because it entails giving third parties a way to access data provider information systems and initiate payments in a way that can impede data providers' efforts to monitor them.

Impacts of These Challenges on the Open Banking System

The challenges described above in this part I.C have impeded progress in negotiating access agreements in several respects. Data providers may decide not to establish a developer interface in the first instance, making it difficult for third parties to access data without resorting to screen scraping. Even where data providers have a developer interface, conflicting interests may inhibit parties from reaching access agreements. And even where such agreements are reached, negotiating them has often proved costly, and their terms often vary in key respects that undermine the consistency of data access across the system. For example, the scope of and frequency with which data are made available vary from agreement to agreement. Attempts to standardize or streamline negotiations by publishing model agreements generally have been undertaken only by certain segments of the market, limiting their effectiveness.[25]

These challenges also hamper efforts by industry to establish standards for open banking. The absence of clarity around the scope of consumers' data rights and the appropriate role of various parties has left standard setters to negotiate a thicket of conflicting interests. The result has been standards limited in their scope, specificity, and adoption. These dynamics have limited standard setters from taking on other functions for which they are potentially well-suited, such as apportioning liability and developing an accreditation system.

Due to the lack of progress on access agreements and the establishment of open, fair, and inclusive industry standards, the open banking system has come to depend heavily on a handful of data aggregators. Aggregators currently function as connectors and, as a practical matter, standardize how many third parties receive data. As such, they accrue economic benefits from the system's inability to scale bilateral access agreements 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 developer interfaces 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 in this part I.C are resolved, consumers should be able to safely exercise their data access rights in an open system not dominated by the interests of any one segment of the market.

D. Overview of Rulemaking Objectives

The CFPB is proposing regulations to implement CFPA section 1033. In addition to ensuring consumers can access covered data in an electronic form from data providers, the proposed regulations would address the challenges described above in part I.C with respect to the open banking system by delineating the scope of data that third parties can access on a consumer's behalf, the terms on which data are made available, and the mechanics of data access. The proposed regulations also would ensure that third parties act on consumers' behalf when collecting, using, or retaining data.

If finalized as proposed, this rule will foster a data access framework that is (1) safe, by ensuring third parties are acting on behalf of consumers when accessing their data, including with respect to consumers' privacy interests; (2) secure, by applying a consistent set of security standards across the market; (3) reliable, by promoting the accurate and consistent transmission of data that are usable by consumers and authorized

[23] *See, e.g.,* Off. of the Comptroller of the Currency, *Third-Party Relationships: Interagency Guidance on Risk Management* (June 6, 2023), *https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html.*

[24] Dan Murphy *et al., Financial Data—The Consumer Perspective,* at 15, 18, Fin. Health Network (June 30, 2021), *https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf;* Brooke Auxier, *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/.*

[25] *See, e.g.,* The Clearing House, *The Clearing House Releases Model Agreement to Help Facilitate Safe Sharing of Financial Data* (Nov. 12, 2019), *https://www.theclearinghouse.org/payment-systems/articles/2019/11/model_agreement_press_release_11-12-19.*

third parties; and (4) 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 is intended 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 would promote the use and development of standardized formats.

1. Clarifying Scope of Data Rights

The CFPB is proposing to define key terms, establish which covered persons would be required to make data available to consumers, and define which data would need to be made available to consumers. As discussed in part IV.A, the CFPB is proposing to first apply part 1033 to a subset of covered persons—namely, entities providing asset accounts subject to the Electronic Fund Transfer Act (EFTA) [26] and Regulation E,[27] credit cards subject to the Truth in Lending Act (TILA) [28] and Regulation Z,[29] and related payment facilitation products and services. This proposed scope is intended to prioritize some of the most beneficial use cases for consumers and leverage data providers' existing capabilities. The proposed definition of covered data would ensure consumers have access to key pricing terms, transaction and balance information, payment initiation information, and terms and conditions. As discussed in part IV.B, this would facilitate consumer choice, including the ability of consumers to change providers of products or services. Clarifying the scope of the data right also would promote consistency in the data made available to consumers, reduce costs of negotiating the inclusion of such data in access agreements, and focus the development of technical standards around such data.

2. Establishing Basic Standards for Data Access

As discussed in part IV.C, the proposed rule would require data providers to establish and maintain a developer interface for third parties to access consumer-authorized data. Developer interfaces would need to make available covered data in a standardized format, in a commercially reasonable manner, without unreasonable access caps, and pursuant to certain security specifications. In addition, data providers would need to follow certain procedures to disclose information about themselves and their developer interfaces, which would ensure that consumers and authorized third parties have information necessary to make requests and use the developer interface. Data providers also would be required to establish and maintain certain written policies and procedures to promote these objectives. Altogether, these provisions would ensure data providers make data available reliably, securely, and in a way that promotes competition.

3. Transitioning the Market From Screen Scraping

The proposed rule would prevent data providers from relying on screen scraping to comply with the proposal because it is not a viable long-term method of access for the reasons discussed in part I.C above. Instead, data providers would be required to establish and maintain developer interfaces that would make data available in a machine-readable, standardized format and could not allow a third party to access the system using consumer interface credentials. These provisions would help the market move away from screen scraping, even outside of the product markets covered under the proposed rule. Once developer interfaces have been established by data providers with respect to covered data, it will be more efficient for these data providers to provide access to other data types via the same developer interface. And, as the infrastructure for establishing and using developer interfaces embeds itself in the market for accessing consumer financial data, data providers outside the scope of the proposed rule will face competitive pressure to adopt and use developer interfaces as well. 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 (*e.g.,* through a developer interface). If so, the CFPB would consider using the tools at its disposal to address this topic in advance of the proposed compliance dates.

4. Clarifying Mechanics of Data Access

As discussed in part IV.C, the CFPB is proposing certain requirements and clarifications to implement CFPA section 1033 with respect to when a data provider must make available covered data upon request to consumers and authorized third parties. These proposed provisions address how a data provider can manage requests for third parties to access a developer interface and when a data provider must respond to requests for information through a consumer and developer interface. While the CFPB is not proposing amendments to Regulation E at this time, proposed part 1033 contains multiple provisions that would reduce fraud and unauthorized access risk in the open banking system. These provisions include requiring that third party access be effected through a developer interface (rather than through credential-based screen scraping); prohibiting a developer interface from requiring a third party to obtain or possess credentials for the consumer interface; and allowing data providers to share tokenized account and routing numbers. The proposed rule would allow data providers to restrict access to their developer interface when they have reasonable risk management grounds to do so.

5. Ensuring Third Parties are Acting on Behalf of Consumers

To effectuate consumers' control of access to their data, the proposed rule contains provisions intended to ensure that when consumers authorize a third party to access data on their behalf, the third party is actually doing so. To that end, the proposed rule would require a third party to 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 would aim 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 include 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.

Separately, the proposed rule would exercise the CFPB's authority to define financial products or services under the CFPA to ensure that it includes providing financial data processing. Although the CFPB has tentatively concluded that this activity would

[26] 15 U.S.C. 1693 *et seq.*

[27] 12 CFR part 1005.

[28] 15 U.S.C. 1601 *et seq.*

[29] 12 CFR part 1026.

qualify as a financial product or service without a CFPB rule, this rule provision 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.

6. Promoting Fair, Open, and Inclusive Industry Standards

Industry standard-setting bodies that operate in a fair, open, and inclusive manner have a critical role to play in ensuring a safe, secure, reliable, and competitive data access framework. Accordingly, indicia of compliance with various provisions in the rule, if finalized as proposed, would include conformance with standards promulgated by fair, open, and inclusive standard-setting bodies recognized by the CFPB.

Comprehensive and detailed technical standards mandated by Federal regulation could not address the full range of technical issues in the open banking system in a manner that keeps pace with changes in the market and technology. A rule with very granular coding and data requirements risks becoming obsolete almost immediately, which means the CFPB and regulated entities would experience constant regulatory amendment, or worse, the rule would lock in 2023 technology, and associated business practices, potentially for decades. In developing the proposal, the CFPB is mindful of these limitations and the risk that they may adversely impact the development and efficient evolution of technical standards over time. In contrast, industry standards appropriately developed within the CFPB's proposed data access framework would not be subject to these limitations.

To help support and maintain a data access framework that enables consumer access in a consistently safe, reliable, and secure manner across the market, industry standards must be widely adopted. To meaningfully scale, standards must reflect a diverse set of interests, increasing the likelihood that market participants will adopt the standards and maintain their integrity. Conversely, if standards are controlled by dominant incumbents or intermediaries, they may enable rent-extraction and cost increases for smaller participants. Fair, open, and inclusive standard-setting bodies are vital to promote standards that can support a data access system that works for consumers, rather than the interests of dominant firms.

E. Applicability of Other Laws

1. Electronic Fund Transfer Act

This proposed rule would not alter a consumer's statutory right under EFTA to resolve errors through their financial institution. Regulation E financial institutions—including digital wallet 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. Consumers are protected from liability from these unauthorized transfers under EFTA and Regulation E, although the relevant financial institution may be able to seek reimbursement from other parties through 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 financial institution is entitled to reimbursement from the originating depository institution that initiated the unauthorized payment.

Various stakeholders have 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 proposing 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, and implementing authorization procedures for third parties that would require they commit to data limitations and compliance with the Gramm-Leach-Bliley Act (GLBA) [30] Safeguards Framework. These provisions are intended to drive market adoption of safer data sharing practices.

2. Fair Credit Reporting Act

As described above, entities engaged in data aggregation activities play a role in the open banking system by transmitting consumer-authorized data from data providers to third parties. When the data bears on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living and is used or expected to be used, or collected, for ''permissible purposes'' as defined by the FCRA, such as when a third party uses the data to underwrite a loan to a consumer, and when the entity, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating such data for the purpose of furnishing reports containing the data to third parties (and uses any means or facility of interstate commerce to prepare or furnish such reports), the data aggregator is regulated as a consumer reporting agency under the FCRA.

II. Legal and Procedural Background

In 2010, Congress passed the CFPA, including section 1033. This is the first proposed CFPB rule under section 1033.

A. Small Business Advisory Review Panel

Pursuant to the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA),[31] the CFPB issued its Outline of Proposals and Alternatives under Consideration for the Required Rulemaking on Personal Financial Data Rights (Outline or SBREFA Outline).[32] The CFPB convened a SBREFA Panel for this proposed rule on February 1, 2023, and held two Panel meetings on February 1 and 2, 2023.[33] Representatives from 18 small businesses were selected as small entity representatives for this SBREFA process. These entities represented small businesses that would likely be directly affected by a CFPA section 1033 rule. On March 30, 2023, the Panel completed the Final Report of the Small Business Review Panel on the CFPB's Proposals Under Consideration for the Required Rulemaking on Personal Financial Data Rights Rulemaking (Panel Report or SBREFA Panel Report). The CFPB released the Panel Report on

[30] 15 U.S.C. 6801 *et seq.*

[31] Public Law 104–121, 110 Stat. 857 (1996).

[32] 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.*

[33] The Panel consists of a representative from the CFPB, the Chief Counsel for Advocacy of the SBA, and a representative from the Office of Information and Regulatory Affairs in OMB.

April 3, 2023.[34] The CFPB invited other stakeholders to submit feedback on the SBREFA Outline by January 25, 2023.[35] The CFPB has considered the feedback it received from small entity representatives, the findings and recommendations of the Panel, and the feedback from other stakeholders in preparing this proposed rule.

B. Other Stakeholder Outreach

In the years leading up to the release of this proposed rule, the CFPB held a number of outreach meetings with financial institutions, trade associations, nondepositories, aggregators, community groups, consumer advocates, researchers, and other stakeholders regarding the CFPA section 1033 rule, and about the open banking system generally. Findings from such market monitoring activities inform the CFPB on the state of the open banking system.

In January 2023, the CFPB issued two sets of CFPA section 1022(c)(4) market monitoring orders to collect information related to personal financial data rights—one set of orders was sent to a group of data aggregators (Aggregator Collection);[36] the second to a group of large data providers (Provider Collection).[37] The information gathered through these orders informs this proposed rule, including the CFPA section 1022(b) analysis in part VI below.

The CFPB regularly hears from several advisory committees on emerging trends and practices in the consumer financial marketplace and engages with advisory committee members in different formats, including non-public and public engagements. In November 2022, the CFPB Director and CFPB staff engaged in a discussion about data privacy in the context of CFPA section 1033 with members of the Consumer Advisory Board. Additionally, the CFPB Director and CFPB staff received two briefings related to the CFPA section 1033 rule—one from the Consumer Advisory Board and one from the combined Community Bank Advisory Council and Credit Union Advisory Council.[38]

Prior to issuing this proposed rule (in accordance with CFPA sections 1033(e) and 1022(b)(2)(B), and as recommended by the SBREFA Panel), the CFPB consulted on several occasions with staff from the prudential regulators and the FTC to discuss various aspects of this proposed rule. Specifically, the CFPB met with staff from the Board of Governors of the Federal Reserve System, the OCC, the FDIC, the NCUA, the FTC, the Department of Treasury's Bureau of the Fiscal Service, the United States Department of Justice, and the Financial Crimes Enforcement Network. The CFPB also met with a number of State regulators and an association of State regulators to discuss the CFPB's proposals under consideration. The CFPB also met with its foreign counterparts to discuss open banking frameworks in their respective countries.

III. Legal Authority

The CFPB is issuing this proposed rule pursuant to its authority under the CFPA. This part includes a general discussion of several CFPA provisions on which the CFPB relies in this proposed rule.[39] As set forth in section 1021 of the CFPA, Congress established the CFPB to ensure that ''all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.'' Congress also authorized the CFPB to exercise its authorities under Federal consumer financial law, including the CFPA, to ensure that, with respect to consumer financial products and services, consumers have ''timely and understandable information to make responsible decisions about financial transactions,'' ''consumers are protected from unfair, deceptive, or abusive acts and practices and from discrimination,'' that ''markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation,'' and that ''Federal consumer financial law is enforced consistently without regard to the status of a person as a depository institution in order to promote fair competition.''

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 readily makes available covered data in an electronic form usable by consumers and third parties acting on behalf of consumers, upon request, including authorized third parties offering competing products and services. 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 would 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,

[34] 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 SBREFA, the CFPB considers the Panel's findings in its IRFA, as set out in part VII below.

[35] *See https://www.regulations.gov/document/CFPB-2023-0011-0001/comment* (last visited Aug. 28, 2023). Feedback from these other stakeholders was not considered by the Panel and is not reflected in the Panel Report.

[36] Consumer Fin. Prot. Bureau, *Generic Order for Data Aggregators, https://files.consumerfinance.gov/f/documents/cfpb_generic-1022-order-data-aggregator_2023-01.pdf* (last visited Aug. 28, 2023).

[37] Consumer Fin. Prot. Bureau, *Generic Order for Data Providers, https://files.consumerfinance.gov/f/documents/cfpb_generic-1022-order-data-provider_2023-01.pdf* (last visited Aug. 28, 2023).

[38] *See* Consumer Fin. Prot. Bureau, *Consumer Advisory Board Meeting* (Nov. 2, 2022), *https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_consumer-advisory-board-meeting_summary_2022-11.pdf;* Consumer Fin. Prot. Bureau, Cmty. Bank Advisory Council & Credit Union Advisory Council, *Combined Advisory Councils Meeting* (Nov. 3, 2022), *https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_combined-advisory-board-meeting_summary_2022-11.pdf.*

[39] Part IV contains additional material on these authorities.

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.[40] Accordingly, in issuing the proposed rule, the CFPB is exercising its authority under CFPA section 1022(b) to prescribe rules that carry out the 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 when final. 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.''

CFPA section 1022(b)(3)(A) generally provides that the CFPB, by rule, may conditionally or unconditionally exempt any class of covered persons, service providers, or consumer financial products or services, from any provision of the CFPA, or from any rule issued under the CFPA, as the CFPB determines necessary or appropriate to carry out the purposes and objectives of the CFPA, taking into consideration several factors. For a discussion of the CFPB's proposed use of this authority, see the discussion in part IV.A. The statutory language indicates that the CFPB should evaluate the case for creating such an exemption in light of its general purposes and objectives as Congress articulated them in section 1021 of the CFPA, as described above.

C. CFPA Section 1032

CFPA section 1032(a) provides that the CFPB may prescribe rules to ensure that the features of any consumer financial product or service, both initially and over the term of the product or service, are fully, accurately, and effectively disclosed to consumers in a manner that permits consumers to understand the costs, benefits, and risks associated with the product or service, in light of the facts and circumstances. Under CFPA section 1032(a), the CFPB is empowered to prescribe rules regarding the disclosure of the ''features'' of consumer financial products and services generally. CFPA section 1032(c) provides that, in prescribing rules pursuant to CFPA section 1032, the CFPB shall consider available evidence about consumer awareness, understanding of, and responses to disclosures or communications about the risks, costs, and benefits of consumer financial products or services.

D. 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 proposing to exercise this authority in proposed § 1001.2(b).

IV. Discussion of the Proposed Rule

12 CFR Part 1033

A. Subpart A—General

1. Overview

Proposed subpart A would establish the coverage and terminology necessary to implement CFPA section 1033 for this proposed rule, beginning with proposed § 1033.101, which would describe the authority, purpose, and organization of the regulation in proposed part 1033. It contains defined terms appearing throughout the regulatory text, which are described in this part IV.A and elsewhere in part IV and sets forth tiered compliance dates to provide appropriate flexibility to smaller institutions in implementing the rule's requirements.

2. Coverage of Data Providers (§ 1033.111(a) Through (c))

Regulation Z Card Issuers, Regulation E Financial Institutions, and Other Payment Facilitation Providers

In this first proposed rule to implement CFPA section 1033(a), the CFPB is proposing to define a subset of covered persons and consumer financial products or services that would be required to make data available under section 1033(a) of the CFPA. The proposed rule would cover the following consumer financial products or services, as defined at proposed § 1033.111(b)(1) through (3)—generally, 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 latter category—products or services that facilitate payments from a Regulation E account or a Regulation Z credit card—would be intended to clarify that the proposed rule would cover all consumer-facing entities involved in facilitating the transactions the CFPB intends to cover.

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. 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. In addition, digital wallet providers hold 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 that were originally issued by other institutions (sometimes referred to as pass-through payments).

The CFPB has preliminarily determined that the marginal burden of including other payment facilitation products and services would be minimal given how these providers would generally already be covered as Regulation E financial institutions. Digital wallet providers and entities that refer to themselves as neobanks generally qualify as Regulation E financial institutions and sometimes also may be Regulation Z card issuers. Adopting a broad definition could help avoid creating unintentional loopholes as the market evolves.

Covering Regulation E asset accounts, Regulation Z credit cards, and payment facilitation products and services would have additional benefits. This coverage would leverage existing infrastructure for consumer-authorized data sharing, which would facilitate implementation. Data providers generally share the

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

covered data described in this proposed rule on consumer interfaces today, and some share covered data with third parties. Additionally, given the current level of data sharing associated with these products and services, the proposed coverage would prioritize these data for greater protection compared to what is available today. In particular, consumers' payment data can be used to access consumer funds or track household spending. As discussed in part I.D, this proposal would include a number of measures to foster a safe and secure data access framework.

The SBREFA Panel recommended that the CFPB consider clarifying the types of products that would be covered under the proposed rule.[41] In addition, the CFPB received feedback from small entity representatives and other stakeholders indicating confusion about whether the CFPB intended to cover nondepository data providers and their products, and whether all credit card products would be included.

Consistent with the Panel recommendation and the feedback received, the proposal would make clear that a data provider generally would have obligations to make available covered data with respect to a covered consumer financial product or service. Proposed § 1033.111(b) would 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. Proposed § 1033.111(c) would define data provider to mean (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. Proposed example 1 to § 1033.111(c) explains that a digital wallet provider is a data provider. The CFPB requests feedback on the proposed definitions, including whether any further clarification is needed to demonstrate that entities that refer to themselves as neobanks, digital wallet providers, and similar nondepository entities would qualify as data providers.

Other Consumer Financial Products and Services

Today, covered persons typically share information concerning financial products and services that would not fall within the definition of covered data in proposed § 1033.211, such as mortgage, automobile, and student loans. Similar to the payment data that would be covered, information about these products is generally shared through consumer interfaces and supports a variety of beneficial use cases. A significant difference is that this information does not typically support transaction-based underwriting across a range of markets or payment facilitation. Accordingly, the CFPB has preliminarily concluded that prioritizing Regulation E accounts, Regulation Z credit cards, and payment facilitation products and services in this proposed rule could serve to advance competition goals across a broader range of markets. The CFPB intends to implement CFPA section 1033 with respect to other covered persons and consumer financial products or services through supplemental rulemaking.

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 has received feedback from small entity representatives and other stakeholders that there can be limitations to the availability of EBT-related data and that third party access to EBT data could address these issues. EBT cards are exempt from EFTA coverage by statute; pursuant to the Consolidated Appropriations Act of 2023, the U.S. Department of Agriculture has been directed to engage in a rulemaking and issue guidance on EBT card security practices.[42]

The CFPB is considering whether to add EBT-related data to the final rule, or whether to reach EBT cards in a subsequent rulemaking. While EBT cards differ from the current scope of data types included in the proposed regulation in some ways, they have some significant similarities, including that they are used by consumers to make regular purchases. The CFPB requests 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 section 1033. The CFPB also seeks comment on third party practices related to consumer-authorized EBT data, including the interaction between those practices and the limitations on uses that are not reasonably necessary in proposed § 1033.421(a) and (c). Finally, the CFPB seeks comment on the benefits and drawbacks of enabling third party access to EBT-related data, including with respect to data security.

3. Excluded Data Providers (§ 1033.111(d))

Pursuant to CFPA section 1022(b)(3), proposed § 1033.111(d) generally would exempt data providers (as defined in proposed § 1033.111(c)) from the requirements of the proposed rule if they have not established a consumer interface as of the applicable compliance date. Proposed § 1033.131 would define consumer interface as an interface that a data provider maintains to receive requests for covered data and make available covered data in an electronic form usable by consumers in response to the requests. The term is intended to encompass consumer-facing digital banking interfaces that allow consumers to make requests for information, as described in part I.A above.

While the vast majority of banks and credit unions offer consumer interfaces, such as online banking or mobile banking applications, a small number of depository institutions do not offer any such service. For example, among credit unions with fewer than 1,000 deposit accounts, only 21 percent offer online banking services.[43] These institutions tend to be very small and may not have adequate resources to support or maintain these online or mobile banking systems. They may also use a relationship banking model and have a more personalized relationship with their customers.[44]

Some depositories do not offer digital banking in the current environment, despite the ubiquity of computers and smartphones, broad consumer utilization of online banking and mobile banking applications, and the impact of the COVID–19 pandemic, which impeded many consumers' access to

[41] SBREFA Panel Report at 42.

[42] Public Law 117–328, 136 Stat. 5985 (2022).

[43] CFPB calculations based on NCUA data. For details on data see part VII.B.6.

[44] *See, e.g.,* Consumer Fin. Prot. Bureau, *Request for Information Regarding Relationship Banking and Customer Service* (June 14, 2022), *https://www.federalregister.gov/documents/2022/07/20/2022-15243/request-for-information-regarding-relationship-banking-and-customer-service.*

traditional banking channels. This suggests that, first, such entities have not found that the business reasons to provide these services justify the associated costs; and, second, that their customers have not switched to institutions that do provide digital banking services, indicating that such services may not be an important factor for such customers when choosing where to deposit or borrow money.[45] The CFPB notes that it has preliminarily determined to limit this proposed exclusion to depositories that qualify as financial institutions under Regulation E or as card issuers under Regulation Z. Not all CFPA-covered persons will necessarily have the same incentives to facilitate direct customer service with consumers. For example, there may be covered persons that do not market to or contract with consumers and that do not have the same incentives to invest in customer service.

The SBREFA Panel recommended that the CFPB consider whether to create complete or partial exemptions for data providers, or whether to delay implementation for certain data providers for certain aspects of the proposed rule, such as a requirement to establish a developer interface.[46] The Panel also recommended that the CFPB seek comment on how to define potential exemption eligibility requirements or implementation tiers, such as by establishing a threshold based on asset size or activity level, or by exempting data providers based on entity type.[47] Consistent with these recommendations, the CFPB considered whether to exempt all data providers, not just certain depository institutions, that do not provide a consumer interface and, if so, how to structure such an exemption. However, the complicating factors that exist for these types of depository institutions may be less likely to exist for these types of nondepository institutions. For example, nondepository data providers within the scope of the proposed rule tend to be institutions whose business models are built upon providing interfaces to consumers. This is not the case for depository institutions that do not provide an interface for their customers. The CFPB requests comment on whether there are nondepositories that do not provide an interface for their customers, and if so, whether an exemption should include them. The CFPB also seeks comment on whether it should require any exempt depositories to make covered data available in a non-electronic form.

As noted in the discussion of the proposed rule's compliance dates, the CFPB is proposing to provide a longer compliance period for the smallest depository institution data providers. The CFPB also considered not proposing an exemption for any data providers, and instead simply giving some data providers more time to comply. However, because of the dynamics with respect to depository institutions that do not provide an interface for their customers, the compliance burden on these entities would most likely outweigh the marginal benefit of the rule covering an additional very small set of consumer accounts.

The proposed rule would not provide a grace period for depository institutions that do not have a consumer interface as of the effective date but subsequently offer such an interface to their customers. The CFPB requests comment on whether such depositories should be offered some grace period to achieve compliance. Proposed § 1033.111(d) would not exempt depositories that stop providing a customer interface after the effective date. Such depositories possessed the ability to provide an interface for their consumers, and so should remain subject to the rule.

Under CFPA section 1022(b)(3)(A), the CFPB may exercise exemption authority as it determines necessary or appropriate to carry out the purposes and objectives of CFPA section 1033, taking into consideration, as appropriate: (1) the total assets of the class of covered persons; (2) the volume of transactions involving consumer financial products or services in which the class of persons engages; and (3) existing provisions of law which are applicable to the consumer financial product or service and the extent to which such provisions provide consumers with adequate protections.

The CFPB has preliminarily determined that the proposed exemption would promote the CFPB's objectives, discussed in part I above, to ensure that the markets for consumer financial products and services operate transparently and efficiently to facilitate access, as well as its objective to ensure that consumers are provided with timely and understandable information to make responsible decisions about financial transactions. The CFPB has also preliminarily determined that the proposed exemption would promote the CFPA's purpose of ensuring that markets for consumer financial products and services are competitive. As noted above, the depository institutions that would be exempt from the proposed rule's requirements tend to be very small institutions that may not be as technologically sophisticated as larger institutions and likely do not have the resources to support or maintain the interfaces that would be required by the proposed rule. Subjecting these institutions to the proposal could significantly disrupt their businesses, potentially threatening access to consumer financial products and services and reducing competition for consumer financial products and services—both contrary to carrying out the objectives of CFPA section 1033.

The CFPB acknowledges that some consumers would not be given the benefits provided by the proposed rule if these entities were exempt. However, as noted above, these small depository institutions generally provide timely and understandable information through ongoing personal relationships to assist customers in making decisions about financial transactions. The CFPB seeks comment on whether the exclusion for depository institutions that do not provide an interface for their customers should be limited solely to the provision of the interfaces required by the proposed rule, or whether the rule should still require such institutions to comply with the general obligations outlined in proposed § 1033.201(a) and allow flexible compliance with this section. The CFPB also seeks comment on 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 exempt from the proposed rule.

As noted above, the CFPB considers, as appropriate, the applicable statutory factors in CFPA section 1022(b)(3)(A). Because the requirements of this proposed rule would focus on consumers' data, a suitable proxy for considering two of the three factors—total assets of the class of covered persons and the volume of transactions—would be the number of accounts exempted. The CFPB expects the number of data requests will be approximately proportional to the number of accounts. By exempting depository institutions that do not have an interface, the proposed rule would exempt approximately 0.64 percent of total deposit accounts, a very small percentage of deposit accounts covered by the proposed rule.

[45] *See, e.g.,* Miriam Cross, *Credit Unions Podcast: A tiny credit union's tall order,* Am. Banker (May 25, 2023), *https://www.americanbanker.com/podcast/a-tiny-credit-unions-tall-order* (discussing factors some customers of very small credit unions use when determining whether to continue to patronize such institutions).

[46] SBREFA Panel Report at 43.

[47] *Id.* at 42.

This exemption would treat some depository data providers differently than nondepository ones. However, nondepository data providers within scope of this proposed 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, in contrast to depository institutions that have not established a consumer interface for their customers. Thus, the CFPB preliminarily concludes that these two groups are not similarly situated for purposes of this proposed rule. By exempting these depository institutions from regulations that would be more costly and burdensome for them than it would be for their peers with greater technological capabilities, the CFPB would be promoting fair competition.

The CFPB's preliminary determination regarding exempting depository institution data providers that do not provide a consumer interface to their customers is specific to this proposed rule and the data that would be covered by it. Further rulemaking under section 1033 of the CFPA may make different determinations based upon the types of data providers and types of data covered.

4. Compliance Dates (§ 1033.121)

Proposed § 1033.121 would stagger dates by which data providers need to comply with proposed §§ 1033.201 and 1033.301 (the obligations to make data available and establish interfaces) into four distinct tiers to ensure timely compliance with the rule's requirements. From the SBREFA process and other stakeholder feedback, the CFPB understands that a number of factors may affect how quickly a data provider could comply with the proposed rule. These include, for example, a data provider's size, relative technological sophistication, use of third party service providers to build and maintain software and hardware systems, and, in the case of many data providers, the existence of multiple legacy hardware and software systems that impact their ability to layer on new technology.[48] Many smaller depository data providers will need to rely on cores and other third party service providers to create interfaces required by the proposed rule.[49] These entities may experience significant wait times since many other entities may be relying on the same providers for the development of their interfaces.[50] If a depository institution data provider builds its own interface without the assistance of a third party service provider, it may need additional time to do so.

The CFPB preliminarily believes nondepository data providers do not have the same obstacles with respect to compliance as depository institutions because they do not have as many vendors and information technology systems that would need to be connected, and implementation could occur in-house.[51] Thus, these data providers would be able to move more quickly to implement the proposed rule's requirements.

The SBREFA Panel made several recommendations related to compliance dates. Generally, the Panel recommended that the CFPB seek comment on ways to facilitate implementation for small entities, and on implementation options that reduce impacts on small entities, including staging implementation based on categories of data to be made available, entity size, or other factors.[52] The Panel also recommended that the CFPB continue to study the time needed for vendors to establish a data portal on behalf of data providers, as well as the time needed by data providers, data aggregators, and data recipients to integrate into data portals at the scale envisioned by the proposal.[53] Lastly, the Panel recommended that the CFPB consider whether to delay implementation for certain data providers for certain aspects of the rule, such as a requirement to establish a third party access portal, and should seek comment on how to define implementation tiers, such as by establishing a threshold based on asset size or activity level.[54] (The CFPB is proposing to define and use the term developer interface in lieu of the SBREFA Outline's ''third-party access portal.'')

The CFPB considered a number of alternatives to the four tiers outlined in the proposed rule. One option was to have the same compliance date for all data providers. For the reasons discussed in this part IV.A, the CFPB has preliminarily determined that it is necessary to provide some data providers with a longer compliance period than others. The CFPB has preliminarily determined that the proposed exemption combined with the tiered compliance dates based on asset size or revenue appropriately balances the need to provide relief to the smallest data providers that may not be as technologically sophisticated as larger providers while providing a longer timeline for compliance to entities that may need more time. The CFPB also considered basing the compliance tiers on an institution's number of accounts/activity level, rather than asset size or revenue. With respect to number of accounts, the CFPB has preliminarily determined that, because of the breadth of types of data providers and services covered by the proposed rule, it would be difficult to define accounts to properly segment data providers into appropriate tiers, and asset size and revenue provide more precise metrics in which to separate compliance tiers.

Subject to a data provider's ability to deny access, as described in § 1033.321, and the exclusion for data providers described in proposed § 1033.111(d), proposed § 1033.121 would require data providers to grant access to the interfaces required by proposed § 1033.301 to consumers and third parties by four applicable compliance dates based on asset size or revenue, depending on the type of data provider. Under proposed § 1033.121(a), the first compliance date would occur approximately six months after publication of the final rule in the **Federal Register** and would apply to depository institutions that hold at least $500 billion in total assets, and to nondepository institutions that generate at least $10 billion in revenue in the preceding calendar year or are projected to generate at least $10 billion in revenue in the current calendar year. The CFPB uses the term ''total assets'' to make clear that this amount is based upon the total consolidated assets of the institution as reported in published financial statements, as used by the FFIEC.[55] Under proposed § 1033.121(b), the second compliance date would occur approximately one year after **Federal Register** publication and would apply to depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets, and to nondepository institutions that generate less than $10 billion in revenue in the preceding calendar year and are projected to generate less than $10 billion in revenue in the current calendar year. The CFPB has preliminarily determined that placing all nondepository data providers in the first two tiers for compliance appropriately balances the need to provide data providers enough time for compliance with depository data

[48] *Id.* at 36.

[49] *Id.* at 36–37.

[50] *Id.* at 36.

[51] *Id.* at 38.

[52] *Id.* at 46.

[53] *Id.*

[54] *Id.* at 43.

[55] *See, e.g.,* Fed. Fin. Insts. Examination Council, *Large Holding Companies, https://www.ffiec.gov/npw/Institution/TopHoldings* (last visited Sept. 22, 2023).

providers potentially needing additional time. Under proposed § 1033.121(c), the third compliance date would occur approximately 2.5 years after **Federal Register** publication and would apply to depository institutions that hold at least $850 million but less than $50 billion in total assets. Finally, under proposed § 1033.121(d), the fourth and final compliance date would occur approximately four years after **Federal Register** publication and would apply to depository institutions with less than $850 million in total assets.

The CFPB seeks comment on whether different or additional criteria, such as an institution's number of accounts or other criteria, should be taken into consideration when determining compliance dates. The CFPB also seeks comment on the structure of each tier, and whether nondepository institutions should be included in all four tiers.

The CFPB recognizes that data providers may need to transition third parties to developer interfaces in a staggered order. Under the proposed rule, a data provider not excluded from coverage could delay a third party's access to an interface in accordance with proposed § 1033.321. The CFPB seeks comment on whether the proposed rule provides data providers sufficient flexibility for such a transition or whether revisions to the proposed rule or additional guidance is needed. For example, the CFPB seeks comment on whether the final rule should include language clarifying that data providers should be granted any period of time to fully transition third parties to the interfaces that would be required under proposed § 1033.301 to ensure that data providers do not impede timely third party access to an interface while accounting for reasonable risk management concerns.

5. Third Party, Authorized Third Party, Consumer, and Data Aggregator (§ 1033.131)

The CFPB is proposing that a third party acting on behalf of a consumer would be able to access covered data. Proposed § 1033.131 includes several definitions that are used in describing the proposed processes and conditions for a third party to access covered data on behalf of a consumer. The CFPB is proposing these definitions to carry out the objectives of CFPA section 1033.

The CFPB is proposing 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 uses the term third party to refer to entities seeking access to covered data and to other parties, including data aggregators.

As discussed in part III above, the CFPB interprets CFPA section 1033(a) to require data providers to make available covered data to certain third parties ''acting on behalf'' of a consumer. The CFPB is proposing 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, discussed in part IV.D, specifies what requirements a third party must satisfy to become an authorized third party that is entitled to access covered data on behalf of a consumer.

The CFPB is proposing 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. As discussed below, some third parties retain data aggregators for assistance in obtaining access to data from data providers. The proposed rule includes certain provisions in proposed § 1033.431 that specify 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 requests comment on whether data aggregator is an 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.

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

6. Qualified Industry Standard (§§ 1033.131 and 1033.141)

As discussed in part I.D, fair, open, and inclusive industry standards are a critical element in the maintenance of an effective and efficient data access system. To promote the development of such external standards, the CFPB is generally proposing throughout part 1033 that indicia of compliance with certain provisions include conformance to an applicable industry standard issued by a fair, open, and inclusive standard-setting body. Proposed §§ 1033.131 and 1033.141 would carry out the objectives of CFPA section 1033 by encouraging the development of fair, open, and competitive industry standards that would satisfy certain provisions of the proposed rule. The CFPB also is proposing §§ 1033.131 and 1033.141 pursuant to its authority under CFPA sections 1022(b)(1) and 1033(d).

Proposed § 1033.131 would define the term qualified industry standard to mean a standard that is issued by a standard-setting body that is fair, open, and inclusive. In turn, proposed § 1033.141 provides that a standard-setting body is fair, open, and inclusive and is an issuer of qualified industry standards when the body has the following attributes: (1) openness (sources and processes used are open to all interested parties, including consumer and other public interest groups, authorized third parties, data providers, and data aggregators); (2) balance (decision-making power is balanced across all interested parties, including consumer and other public interest groups, with no single interest dominating decision-making); (3) due process (publicly available policies and procedures, adequate notice of meetings and standards development, and a fair process for resolving conflicts); (4) an impartial appeals process; (5) consensus (general agreement, not unanimity, reached through fair and open processes); (6) transparency (procedures are transparent to participants and publicly available); and (7) the body has been recognized by the CFPB within the last three years as an issuer of qualified industry standards.

Under this proposed rule, indicia of compliance with a particular rule provision would include conformance to a qualified industry standard. However, an entity does not have to show adherence to a qualified industry standard to demonstrate compliance with a provision of the rule, as long as its conduct meets the requirement of the rule provision. Conversely, adherence to a qualified industry standard would not guarantee that the entity has complied

with the rule provision. There are provisions in the proposed rule that would not mention qualified industry standards at all, generally because their terms do not leave the same room for compliance to be informed by adherence to an external standard.

The one instance in which the proposed rule would take account of external standards in a manner that differs from that described above is the proposed requirement in § 1033.311(b) that data providers use standardized formats. There, the CFPB is proposing that if a data provider's interface makes covered data available in a format that is set forth in a qualified industry standard, then the interface is deemed to satisfy the proposed requirement to use a standardized format. The CFPB is also proposing that a data provider's developer interface would be deemed to satisfy the proposed format requirement if, in the absence of an industry standard, it makes covered data available in a format that is widely used by the developer interfaces of other similarly situated data providers. For certain other proposed requirements, indicia of compliance may include conformance to a qualified industry standard; for this one alone, however, conformance with such a standard would be deemed to constitute compliance. CFPA section 1033(d) requires the CFPB by rule to prescribe standards to promote the development of standardized data formats. Conformance with a qualified industry standard with respect to standardized formats would carry out this objective of CFPA section 1033(d).

To promote a competitive data access framework in which standard-setting bodies do not inappropriately use their position to benefit a single set of interests, the CFPB has preliminarily determined they should reflect a full range of relevant interests—consumers and firms, incumbents and challengers, and large and small actors. The proposed definition would respond to the recommendation of the SBREFA Panel that the CFPB consider to what extent existing external standards for data sharing should inform the proposed rule.[56] In line with the Panel recommendation, the CFPB has preliminarily determined that external standards would reflect the requisite input from the full range of relevant interests, and therefore would properly serve as indicia of compliance with various provisions of proposed part 1033, if the standards were to achieve the status of being a qualified industry standard as defined. A qualified industry standard, by definition, would be developed, adopted, and maintained by a fair, open, and inclusive standard-setting body, and such a body would, per the proposed attributes listed above, necessarily be a body that reflects the full range of relevant interests.

The proposed rule would be agnostic about what specific technical format a data provider must use and would not envision that the CFPB would develop the infrastructure through which data could be processed, as was suggested by a small entity representative.[57] While the CFPB has not ruled out these types of alternatives, the CFPB has preliminarily determined that they could inappropriately stifle ongoing evolution of financial industry data-sharing practices.

The proposed attributes of the qualified industry standard definition would be consistent with longstanding OMB Circular A–119, which addresses Federal participation in the development and use of standards,[58] and which is well accepted by standard-setting experts as setting forth ''a limited set of foundational attributes of standardization activities.'' [59] Nonetheless, the CFPB acknowledges that the open banking system comprises arguably a more diverse and larger set of participants than many other environments to which industry standards might apply. Accordingly, the CFPB requests comment on the adequacy of these proposed attributes for ascertaining whether an open banking standard-setting body is fair, open, and inclusive. In this regard, the CFPB emphasizes that it intends the proposed attributes to pertain only to industry standards and standard-setting bodies; the attributes would not be pertinent with respect to standards issued by governmental standard-setting bodies such as the National Institute of Standards and Technology.

The CFPB's proposed approach to defining qualified industry standards aligns with the statutory purposes and objectives for the CFPB established in section 1021 of the CFPA, which include ensuring that consumer financial markets, such as the market for data sharing, are fair, transparent, competitive, and efficient, and ensuring that Federal consumer financial law is enforced consistently, without regard to the status of a person as a depository institution. Moreover, the proposed industry standard definition would align with the language of CFPA section 1033(e)(3) that rules do not inappropriately ''promote the use of any particular technology.''

CFPB Recognition of Industry Standard-Setting Bodies

Proposed § 1033.141(b) provides that a standard-setting body may request that the CFPB recognize it as an issuer of qualified industry standards. The attributes of fairness, openness, and inclusion listed as factors in proposed § 1033.141(a)(1) through (6) would inform the CFPB's consideration of the request. CFPB recognition would help provide clarity to market participants that a standard-setting body has the necessary attributes of fairness, openness, and inclusion. It would also incentivize standard-setting bodies to devote the resources needed to achieve these attributes by providing them with validation from the CFPB, which would encourage adoption of their standards. The CFPB requests comment on the procedures it should use to recognize standard-setting bodies. For example, the CFPB requests comment on whether it should recognize a given body before, after, or at about the same time as the body seeks to issue a qualified industry standard or whether the recognition procedures should be flexible enough to accommodate all of those possibilities.

The CFPB intends to subsequently provide guidance on the substance of the standards issued by the qualified industry standard-setting bodies recognized by the CFPB. The CFPB requests comment on how to provide guidance and, in particular, on how to ensure that the substance is consistent with the provisions of this proposed rule, as finalized.

B. Subpart B—Obligation To Make Covered Data Available

1. Overview

As discussed in part I.C, disagreements around the types of 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. Proposed subpart B would seek to resolve these questions with respect to how CFPA section 1033(a) applies by establishing a

[56] SBREFA Panel Report at 44.

[57] *Id.* at 28.

[58] OMB Circular A–119 was originally published in 1996; *see https://www.govinfo.gov/content/pkg/FR-1996-12-27/html/96-32917.htm.* The current Circular, effective January 27, 2016, is available at *https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf.*

[59] March 17, 2022 testimony of Dr. James Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, of the Department of Commerce's NIST, before the United States House of Representatives Committee on Science, Space and Technology Subcommittee on Research and Technology, available at *https://www.nist.gov/speech-testimony/setting-standards-strengthening-us-leadership-technical-standards.*

framework for the general categories of data that would need to be made available, including specific data fields that have been significant sources of disagreement, and exceptions from these requirements. Proposed 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.

2. Obligation To Make Covered Data Available (§ 1033.201)

Consistent with the general obligation in section 1033(a) of the CFPA, proposed § 1033.201(a) would 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. These covered data would need to be made available in an electronic form usable by consumers and authorized third parties. Compliance with the requirements in proposed §§ 1033.301 and 1033.311 also would be required.

The CFPB interprets CFPA section 1033(a) to set forth a general obligation to make available data in an electronic form usable by consumers and authorized third parties that is independent of other obligations proposed in subpart C. Even if a data provider fully complied with the requirements of proposed subpart C with respect to consumer and developer interfaces, they might attempt to circumvent the objectives of section 1033 by engaging in other conduct that effectively makes data unavailable or unusable to consumers and authorized third parties. The CFPB requests comment on whether it would be clearer to interpret CFPA section 1033(a) to 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, and (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. Such a provision would carry out the objectives of CFPA section 1033, and would prevent evasion, pursuant to the CFPB's authority under section 1022(b)(1), by ensuring data providers do not engage in conduct not specifically addressed by the proposal but that nonetheless could practically interfere with the exercise of rights under CFPA section 1033(a). The CFPB also requests comment on whether there are specific practices that the proposal should identify that might effectively make data unavailable or unusable to consumers and authorized third parties, other than those already identified in proposed subpart C, such as fees for data access, as discussed with respect to proposed § 1033.301(c), or unreasonable access caps, as discussed with respect to proposed § 1033.311(c)(2).

The CFPB requests comment on whether other language might be appropriate to achieve this objective. For example, section 3022(a) of the Public Health Service Act (PHSA) [60] and implementing regulations promulgated by HHS [61] address the practice of ''information blocking,'' defined, in part, as a practice that ''is likely to interfere with, prevent, or materially discourage access, exchange, or use of'' electronic health information, except as required by law or specified by HHS rule. The CFPB seeks comment on whether this language would be appropriate to include as a general prohibition implementing CFPA section 1033, considering that the market for electronic health information and the applicable legal framework are distinct from the context and authorities applicable to this proposal.

The CFPB also requests comment on whether, instead of proposing to restate CFPA section 1033(a) as setting forth an obligation independent of the specific provisions in proposed subpart C, it should instead interpret CFPA section 1033(a) to mean that a data provider's obligations under the statute are fully satisfied if the data provider complies with all of the requirements of proposed subpart C.

With respect to a data provider's obligation to make available data in its control or possession, proposed § 1033.201(a) would mean a data provider would have to make a consumer's data available in any language maintained in records under its control or possession. For example, a data provider would have to make Spanish and English language records available if account records were maintained in Spanish and English.

The CFPB received questions during the SBREFA process about how current the covered data must be, including whether data providers could simply provide the last monthly statement rather than being required to make available recent transactions and the current account balance. 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. Proposed § 1033.201(b) would interpret 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. For example, a data provider would need to make available information concerning authorized but not yet settled debit card transactions. 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, proposed § 1033.201(b) is not intended to limit a consumer's right to access historical covered data. The CFPB requests comment on whether the provision regarding current data would benefit from additional examples or other clarifications. The CFPB also requests 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.

3. Covered Data (§ 1033.211)

CFPA section 1033(a) generally requires data providers to make available ''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.'' Proposed § 1033.211 would implement this broad language to define the information that a data provider would need to make available under the general obligation in proposed § 1033.201(a). Proposed § 1033.211 uses the term covered data instead of the statutory term ''information'' and defines covered data to mean 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.

Several small entity representatives and other stakeholders raised concerns during the SBREFA process with respect to a proposal the CFPB was considering to require a broader set of data than

[60] 42 U.S.C. 300jj–52.

[61] 45 CFR 171.103; 85 FR 25642 (May 1, 2020).

what would be included in this proposed rule, such as certain payment routing and demographic information that is not typically shared with consumers or third parties. Commenters stated that requiring that this information be made available could introduce new fraud and privacy risks to consumers that do not exist in the market today, would not support particularly beneficial use cases, and could impose significant new burden on data providers as some data are held across multiple information technology systems. Many data provider commenters supported an approach to require data that are already available through digital banking, or otherwise supported the inclusion of periodic statement information.

The SBREFA Panel recommended that the CFPB further consider whether the proposed rule should require data providers to make available all six categories of information set forth in the SBREFA Outline.[62] In considering the types of information that data providers would need to make available, the Panel recommended that the CFPB consider the small entity representatives' feedback on costs to small data providers with respect to the following: accessing data stored with multiple vendors or under the control of other third party service providers; restrictions on data providers' ability to share information; and whether sharing certain information could expose data providers and authorized third parties to legal liability or reputational risk.[63]

The proposed covered data definition would leverage existing operational and legal infrastructure: data providers generally make this covered data available through digital account management and existing laws require most of the proposed categories of information to be disclosed through periodic statement and account disclosure requirements. The CFPB preliminarily concludes that requiring data that is generally made available to consumers today would support most beneficial consumer use cases, including transaction-based underwriting, payment credential verification, comparison shopping, account switching, and personal financial management. The CFPB understands that certain of the proposed categories of information, 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 requests comment on the benefits and data needs for consumers who are in the process of switching accounts.

The proposed covered data definition also would address several issues in the consumer-authorized data sharing system today, including (1) maximizing consumer benefits by clarifying which types of data would be included in the consumer's CFPA section 1033 right; (2) addressing potential data provider anti-competitive conduct and incentives to withhold particular types of data; and (3) promoting conditions for standardization in the market. Currently, data providers have different interpretations of the categories of information that would be included in the proposed covered data definition and provide authorized third parties with inconsistent access to that 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 to data access agreements must negotiate individual categories of information that can be shared.

To address concerns about data providers restricting access to specific pieces of information, the proposed rule also would give examples of information that would fall within the covered data categories. These examples are illustrative and are not an exhaustive list of data that a data provider would be required to make available 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 requests comment on whether additional data fields should be specified to minimize disputes about whether the information would fall within the proposed covered data definition. In addition, the proposed rule would allow flexibility as industry standards develop while minimizing ambiguity over the types of information that must be made available. The CFPB also requests comment on whether the proposed categories of information provide sufficient flexibility to market participants to develop qualified industry standards.

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.

Transaction Information

Transaction information under proposed § 1033.211(a) refers to information about individual transactions, such as the payment amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges. Some bank data providers have provided feedback suggesting that a rule not cover pending transactions. These stakeholders have cited concerns about how the information is subject to change and is not provided on monthly account statements. Some bank data providers have stated that pending transaction information is already provided through online or mobile banking applications today, or otherwise supported including that information. The CFPB preliminarily concludes that pending transaction information supports a variety of beneficial use cases, including fraud detection and personal financial management, and therefore should be included within the proposed covered data definition.

Transaction information also would include historical transaction information in the control or possession of the data provider. Proposed § 1033.211(a) explains that a data provider would be deemed to make available sufficient historical transaction information if it makes available at least 24 months of such information. The CFPB is aware that historical transaction data supports a variety of use cases, including transaction-based underwriting, account switching, and personal financial management. However, data providers do not make a consistent amount of historical transaction information available, so a consumer's ability to access historical data depends on their provider. For example, some nondepository data providers appear to make over five years of historical transaction data available, while some bank data providers limit historical

[62] SBREFA Panel Report at 43.

[63] *Id.*

transaction data to 3, 6, 12, 24, or 30 months.

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 concludes 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 amount 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 understands 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. In the SBREFA Outline, the CFPB considered a data parity approach to historical transaction data, where a data provider would only need to share as much historical transaction data as it makes available through a consumer interface.[64] However, the CFPB is concerned that, in practice, a data parity approach would be difficult to enforce and would leave some consumers without sufficient historical transaction data to support transaction-based underwriting, account switching, and other use cases.

The CFPB requests comment on whether the transaction information examples are sufficiently detailed and consistent with market practices. The CFPB also requests comment on 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 requests 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.

Account Balance

The account balance category would include available funds in an asset account and any credit card balance. The CFPB requests 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.

Information To Initiate Payment To or From a Regulation E Account

This category of information would require a data provider to make available information to initiate a payment to or from the consumer's Regulation E account. The proposed rule explains that this category includes a tokenized account and routing number that can be used to initiate an ACH transaction. In complying with its obligation under proposed § 1033.201(a), 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.

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, 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. 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 argued 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 concludes 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 notes 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 requests 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 requests comment on whether data providers should also be required to make available information to initiate payments from a Regulation Z credit card.

Terms and Conditions

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 would describe several non-exhaustive examples of information that would constitute terms and conditions.

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 is proposing to include APR, annualized percentage yield, fees, and other pricing information in this category. In addition, this provision would benefit consumers because consumers today may not be able to easily find this information through their online or mobile banking applications, and some data providers may not be consistently sharing it with authorized third parties. The CFPB requests comment on whether the final rule should include more examples of information that must be made available under terms and conditions.

Upcoming Bill Information

Upcoming bill information would include bills facilitated through the data provider, such as payments scheduled through the data provider and 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 concludes that this information would be necessary to support personal financial management

[64] SBREFA Outline at 27.

and consumers who are switching accounts. The CFPB seeks comment on whether this category is 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.

Basic Account Verification Information

Basic account verification information would be limited to the name, address, email address, and phone number associated with the covered consumer financial product or service.

The CFPB is aware that certain pieces of identifying consumer information are commonly shared with third parties today for beneficial use cases. For example, a lender may seek to verify that loan funds are being 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 that data providers sometimes limit access to this information, and requested that the CFPB should clarify that account verification information must be shared. However, many small entity representatives and other stakeholders raised significant concerns about the proposed rule covering other identity information that is not typically shared today, such as demographic data, as the beneficial use cases for such information is limited compared to the significant privacy and discrimination risks.

The CFPB preliminarily concludes 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 underwriting 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 has 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 SSNs are shared for some beneficial consumer use cases, like mortgage underwriting. However, the sharing of SSNs is not ubiquitous. The CFPB preliminarily concludes that SSNs may continue to be shared as appropriate but, given the risks to consumers, the proposed rule would not require data providers to make them available.

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

4. Exceptions (§ 1033.221)

The CFPB is proposing in § 1033.221 four exceptions to the requirement to make data available under the proposed rule, along with some clarifications of data that do not fall within these exceptions. These proposed exceptions would implement section 1033(b) of the CFPA by restating the statutory language and providing certain interpretations.

The first exception would cover any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. The CFPB is aware that some data providers have argued that certain account information falls within this exception because such information is an input or output to a proprietary model. The CFPB is proposing to clarify that 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 would cover 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. The CFPB received feedback during the SBREFA process that at least one data provider cited this exception to avoid including general account information, such as the name on the account.[65] To avoid misuse of this exception where information has multiple applications, the CFPB is proposing 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 would cover information required to be kept confidential by any other provision of law. Information would not qualify for this exception merely because a data provider must protect it for the benefit of the consumer. For example, a data provider cannot restrict access to the consumer's own information merely because that information is subject to privacy protections.

The fourth exception would cover any information that a data provider cannot retrieve in the ordinary course of its business with respect to that information.

The proposed definition for covered data in proposed § 1033.211 would include information that is made available to consumers and authorized third parties today or is required to be disclosed under other existing laws. The exceptions proposed in § 1033.221 are narrow, and covered data would not typically qualify for any of these exceptions; note 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.

During the SBREFA process, small entity representatives and other stakeholders provided examples of data that could fall within the exceptions, such as proprietary algorithms or underwriting models, but the examples would not be considered covered data and accordingly would not fall within the scope of the proposed rule. The SBREFA Panel recommended that the CFPB continue to seek feedback on how to interpret these exceptions, and further consider whether there are specific pieces of information that should be covered under any of these exceptions.[66] Consistent with the Panel recommendation, the CFPB requests 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

[65] SBREFA Panel Report at 25.

[66] *Id.* at 43.

pretextual basis. The CFPB intends to monitor the market for pretextual use of the CFPA section 1033 exceptions.

C. Subpart C—Establishing and Maintaining Access

1. Overview

The provisions in proposed subpart C would address some of the significant questions and challenges described in part I.C by clarifying the terms on which data are made available and the mechanics of data access, including basic operational, performance and security standards, and other policies and procedures. In particular, certain provisions would ensure that data providers make covered data available to third parties through a developer interface rather than through the screen scraping of a consumer interface. Other provisions would include procedures to facilitate the ability of third parties to request data and ensure data providers are accountable for their obligations in proposed subpart C. In addition, to prevent data providers from inhibiting consumers' exercise of this statutory right, the CFPB is proposing a bright-line prohibition against data providers charging fees for establishing and maintaining the required interfaces or for receiving requests and making available covered data in response to requests. Together, the provisions in proposed subpart C would contribute to a safe, reliable, secure, and competitive data access framework.

2. General Requirements (§ 1033.301)

Requirement To Establish and Maintain Interfaces (§ 1033.301(a))

The CFPB proposes in § 1033.301(a) to require a data provider subject to the requirements of proposed part 1033 to maintain a consumer interface and to establish and maintain a developer interface. A data provider's consumer interface and developer interface would be required to satisfy the requirements in proposed § 1033.301(b) and (c). The developer interface would be subject to additional requirements in proposed § 1033.311. Proposed § 1033.301(a) would carry out the objectives of CFPA section 1033 by ensuring consumers and authorized third parties can make requests and receive timely and reliable access to covered data in a usable electronic form, and would fulfill other objectives discussed below with respect to proposed §§ 1033.301 and 1033.311, including promoting the development and use of standardized formats.

The terms consumer interface and developer interface are defined in proposed § 1033.131 as interfaces through which a data provider receives requests for covered data and makes covered data available in an electronic form usable by consumers and authorized third parties in response to the requests. Proposed § 1033.111(d) would exclude data providers that do not have a consumer interface from the requirements of proposed part 1033. Thus, proposed § 1033.301(a) would not require a data provider to establish a consumer interface, but only to maintain a consumer interface that the data provider already has.

The CFPB is not aware of significant concerns regarding the ability of consumers to access covered data from consumer interfaces. The CFPB intends for the provisions in the proposed rule applicable to consumer interfaces generally to ensure the continuation of current data provider practices. Based on its market expertise, the CFPB expects that data providers' existing consumer interfaces will generally satisfy the data provider's obligation under proposed § 1033.301(a) to maintain an interface for making covered data available to consumers. The CFPB requests comment on the extent, if any, to which the provisions applicable to consumer interfaces in proposed subpart C would be inconsistent with current practices.

A consumer interface generally would not satisfy a data provider's obligation under proposed § 1033.301(a) to establish and maintain a developer interface, which must satisfy requirements in proposed § 1033.311. These provisions in proposed § 1033.311 are intended, in part, to ensure that data providers do not rely on the screen scraping of a consumer interface to satisfy their obligations under CFPA section 1033(a). As recommended by the SBREFA Panel, the CFPB considered whether screen scraping should be an alternative means of sharing data with third parties in some circumstances.[67] The CFPB is not proposing to require 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. As discussed in part I.C, screen scraping as a whole presents risks to consumers and the market and relying on credential-based screen scraping would complicate the mechanics of data access, particularly with respect to authentication and authorization procedures for data providers. The proposed requirements in subpart C, such as the performance specifications for developer interfaces in § 1033.311(c), would ensure that consumers and authorized third parties have reliable access to consumers' covered data.

As also recommended by the SBREFA Panel, the CFPB considered whether there are forms of screen scraping that would reduce the impact of developer interface service interruptions on third parties and minimize costs to data providers and third parties while ensuring data quality and security.[68] The CFPB has not identified any such forms of screen scraping. Tokenized screen scraping, in which third parties use a tokenized version of a consumer's account credentials, provides data security and consumer control benefits when compared with screen scraping that uses a consumer's account credentials. However, it does not mitigate screen scraping's inherent overcollection, accuracy, and consumer privacy risks, and it would impose costs on data providers in addition to the costs of a developer interface. Additionally, because it would inherently rely on the delivery of unstructured data, permitting data providers to comply with the proposed rule through tokenized screen scraping would not meaningfully advance the statutory mandate to promote the development and use of standardized formats.

In some cases, authorized third parties that are natural persons might have a need to access information in a human-readable form because they lack the means of accessing a developer interface. The CFPB requests comment on how a data provider would make covered data available in a usable electronic form to such authorized third parties.

The SBREFA Panel recommended that the CFPB clarify whether the online financial account management portal that the CFPB was considering with respect to direct access—*i.e.,* a consumer interface—would include a data provider's mobile banking portal in addition to its online banking portal.[69] While both online banking and mobile banking applications could serve as consumer interfaces, proposed § 1033.301(a) would not require that each of the applications satisfy all of the proposed requirements that would apply to consumer interfaces, as long as collectively the two applications satisfy the requirements. The CFPB requests comment on the extent to which data providers currently inform consumers using mobile banking applications that additional information about consumers' accounts may be available

[67] *Id.* at 44.

[68] *Id.*

[69] *Id.* at 43.

through the providers' online banking interfaces.

Machine-Readable Files (§ 1033.301(b))

The CFPB proposes in § 1033.301(b) to require a data provider upon specific request to make covered data available in a machine-readable file that a consumer or authorized third party can retain and transfer into a separate information system. This proposed requirement would apply both to data providers' consumer interfaces and to their developer interfaces. This proposed provision would implement the requirement of CFPA section 1033(a) that covered data be made available in a usable electronic form by ensuring that consumers and authorized third parties can retain electronic files. In addition, the proposed provision would directly implement CFPA section 1033(d).

The proposed provision would allow a data provider to offer additional consumer interfaces that do not satisfy § 1033.301(b) (for example, a smartphone application that does not provide information in a readily printable or downloadable format), as long as the data provider makes covered data available upon request in readily printable or downloadable formats through one of its other consumer interfaces, such as its digital banking interface.

The CFPB preliminarily understands that, as a general matter, existing consumer and developer interfaces typically already provide covered data in a form that would comply with this requirement and may be subject to similar requirements by other applicable laws.[70]

The CFPB therefore has preliminarily determined that the proposed requirement in § 1033.301(b) would impose little or no cost on data providers beyond the cost to establish and maintain a developer interface in the first place; *i.e.,* the proposed requirement would impose little or no cost beyond the cost that would be imposed by proposed § 1033.301(a) (discussed above). The CFPB has also preliminarily determined that proposed § 1033.301(b) would provide important consumer benefits, such as by enabling them to share their data with others, including providers of competing financial products and services.[71]

Fees Prohibited (§ 1033.301(c))

The CFPB proposes in § 1033.301(c) to prohibit a data provider from imposing any fees or charges for establishing or maintaining the interfaces required by proposed § 1033.301(a) or for receiving requests or making available covered data through the interfaces. This provision is proposed pursuant to the CFPB's authority under CFPA sections 1033(a) and 1022(b)(1). The CFPB has preliminarily determined that the prohibition would be necessary and appropriate to effectuate consumers' rights under CFPA section 1033 by ensuring that consumers and authorized third parties are not impeded from exercising consumers' statutory rights because of fees, which would be contrary to the objectives of the statute.

The CFPB notes that proposed § 1033.301(c) would not prohibit a data provider from charging a fee for specific services, other than access to covered data, through the consumer interface. For example, a data provider would not violate the proposed rule if the data provider were to impose a fee for sending an international remittance transfer, which a consumer authorizes and consents to through the consumer interface. Further, the proposed rule would not address account maintenance fees that a data provider might charge to consumers regardless of whether they use the interface.

A data provider that does not already have a developer interface would incur some upfront and ongoing costs to establish and maintain one, and data providers in general will incur some cost to maintain the interfaces as well as a marginal cost of providing covered data through the interfaces. The CFPB has therefore considered whether its proposed rule should permit a reasonable, cost-based fee to recover the upfront or fixed costs associated with establishing and maintaining the interfaces. There also may be some costs associated with providing covered data through the interfaces. The CFPB has preliminarily determined, however, that the marginal cost of providing covered data in response to a request is negligible.

Each data provider is the sole supplier of its customers' financial data and therefore able to exert market power over the prices or fees it charges for authorized access to consumers' data. Data providers have in the past restricted data access for third parties. These restrictions have anti-competitive effects and, by allowing data providers to charge prices for access that are in excess of marginal cost, may harm consumers and third parties. For example, data providers may have an incentive to charge fees in excess of their marginal cost to third parties to make certain competing third party products or services less profitable or less attractive to consumers. In addition, data providers charging different prices to different third parties may also result in competitive harm to consumers and third parties, especially in a market where some data providers have financial interests in third parties they are affiliated with, or act as third parties themselves. Even under circumstances where data providers would not directly gain, price discrimination of this type may distort competition among third parties and harm consumers. Further, prolonged negotiations about fees could delay or obstruct third parties being granted access expeditiously to data providers' developer interfaces, in turn undermining the core consumer data access right. The CFPB requests comment on the above analysis with respect to proposed § 1033.301(c). The CFPB also requests comment on whether any clear and unambiguous set of conditions, limitations, or other parameters exist or should be created 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.

During the SBREFA process, data provider small entity representatives provided feedback that data providers should be permitted to charge fees to third parties for access to covered data.[72] Further, the SBREFA Panel recommended that the CFPB consider how data providers would need to defray the costs associated with developing and maintaining a developer interface.[73] The CFPB will continue to consider this recommendation as it reviews comments on this NPRM and proceeds to develop a final rule. In this regard, the CFPB notes that the proposed rule differs in many respects from the CFPB's proposals under

[70] *See, e.g.,* Cal. Civ. Code sections 1798.100, 1798.130; Va. Consumer Data Prot. Act section 59.1–577 (2023); Colo. Priv. Act section 6–1–1306(1)(e); MRS tit. 10, ch. 1057, section 9607(1)(D); Mass. Info. Priv. & Sec. Act section 10. However, California exempts information subject to the GLBA, and Colorado and Virginia exempt financial institutions subject to the GLBA. Separately, the EU's GDPR requires data portability (Reg. (EU) 2016/679, art. 20, O.J. (L 119) 1 (Apr. 27, 2016)).

[71] *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.*

[72] SBREFA Panel Report at 30.

[73] *Id.* at 44.

consideration at the time the SBREFA Panel provided the above recommendation. Most importantly, the CFPB is now proposing to require data providers to make available a narrower set of covered data than the CFPB was considering at the SBREFA stage. Small data providers generally already make the proposed covered data available through their consumer interfaces. Accordingly, the CFPB expects that it will be relatively low cost for smaller data providers to make covered data available through developer interfaces.

3. Requirements Applicable To Developer Interfaces (§ 1033.311)

As discussed in part I.C, data providers' developer interfaces do not function according to a consistent set of terms, resulting in data that may not be readily usable. In addition, credential-based screen scraping presents security, privacy, and other risks. To foster a safe, reliable, secure, and competitive data access framework, the CFPB is proposing in § 1033.311 additional requirements that would apply specifically to the developer interface described in proposed § 1033.301(a). Proposed § 1033.311(a) would provide that a developer interface required by § 1033.301(a) must satisfy proposed provisions at § 1033.311(b) through (d). These provisions would interpret data providers' obligation to ''make available'' covered data in a ''usable'' electronic form, fulfill the mandate in CFPA section 1033(d) to prescribe by rule standards to promote the use and development of standardized formats, and otherwise carry out the objectives of CFPA section 1033.

Format of Covered Data (§ 1033.311(b))

The CFPB proposes in § 1033.311(b) to require a developer interface to make available covered data in a standardized format. This requirement would implement the mandate in CFPA section 1033(d) that the CFPB prescribe standards to promote the use and development of standardized formats. The interface would be deemed to satisfy this requirement if it makes covered data available in a format set forth in a qualified industry standard (as defined in proposed § 1033.131). In the absence of such a standard, a data provider's interface would be deemed to satisfy proposed § 1033.311(b) 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.

This proposed provision would be intended to ensure that developer interfaces make covered data available in a standardized format that is readily processable by the information systems of third parties across the market, including new entrants and small entities. This proposed provision also is intended to transition the market from relying on screen scraping unstructured data from consumer interfaces.

Consistent with the objectives discussed in part I.D, this provision would seek to foster a reliable and competitive data access framework. Small entity representatives during the SBREFA process indicated that consistent standards would reduce costs for small third parties and small data providers, and would promote competition by reducing integration costs across the market.[74] The SBREFA Panel recommended that the CFPB promote consistency in standards for the availability of information, including the format and transmission of information that data providers make available to third parties.[75] Consistent with that feedback, this provision would seek to ensure that the information systems of, in particular, new-entrant and small-entity third parties can process covered data from the full range of data providers across the market by reducing the extent of varied and idiosyncratic formats that impel reliance on intermediaries to provide data in a usable format.

The CFPB has not determined whether qualified industry standards for data formats presently exist. The proposed rule would seek to accommodate the potential absence of such standards by stating that, in their absence, a data provider could rely on proposed § 1033.311(b)(2) if its developer interface uses a format used by other similarly situated data providers. The CFPB has preliminarily determined that, consistent with CFPA section 1033(a) and (d), requiring 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.

Because proposed § 1033.311(b)(2) would allow data providers across the market to rely on more than one formatting standard, the CFPB acknowledges it would not promote the use and development of a single formatting standard, such as what might be set forth within a qualified industry standard described under proposed § 1033.311(b)(1). The CFPB requests comment on the extent of variation in data formats used for consumer-authorized access today, and the usability of those formats by third parties. The CFPB also requests comment on whether the implementation timelines discussed in part IV.A.4 with respect to proposed § 1033.121 should be adjusted to enable data providers to rely on a standardized format that is set forth in a qualified industry standard as of the applicable compliance date. For example, the CFPB requests comment on whether it should allow for a separate, later compliance date for § 1033.311(b).

Proposed § 1033.311(b)(2) would apply only in the absence of a qualified industry standard. The CFPB requests comment on whether proposed § 1033.311(b)(2) should also be available if there is a qualified industry standard. Alternatively, the CFPB requests comment on whether it should omit proposed § 1033.311(b)(2), meaning that in the absence of a qualified standard only the general requirement under proposed § 1033.311(b) to make available covered data in a standardized format would apply. The CFPB further requests comment on whether there are other approaches that it should deem to comply with § 1033.311(b), instead of or in addition to proposed § 1033.311(b)(1) or (2). Separately, CFPA section 1033(d) does not define the term ''format'' and proposed § 1033.311(b) would not include a definition. The CFPB requests comment on whether a definition is needed and whether format 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.

Commercially Reasonable Performance for Data Providers' Developer Interfaces (§ 1033.311(c)(1))

The CFPB proposes in § 1033.311(c)(1) to require that a data provider's developer interface perform at a commercially reasonable level, and to include provisions regarding what commercially reasonable means. This provision would carry out the objectives of CFPA section 1033 by clarifying how a data provider would make available covered data in a usable form to authorized third parties under CFPA section 1033(a).

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,

[74] *Id.* at 28.

[75] *Id.* at 44.

which many data providers' developer interfaces do not meet. With respect to uniformity, data from the Provider Collection indicated 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. The CFPB has preliminarily determined that the performance of data providers' developer interfaces needs both to improve and to become more consistent and predictable from where that performance is today. In that regard, the CFPB has preliminarily determined that a quantitative minimum performance level would achieve a sufficient level of consistency and predictability.

The CFPB proposes the requirements for commercially reasonable performance of data providers' developer interfaces in proposed § 1033.311(c)(1) pursuant to its authority provided by CFPA section 1033(a) and the CFPB's interpretation of how data providers must make available covered data in an electronic form that is usable by consumers and authorized third parties. Specifically, the CFPB proposes the requirements for commercially reasonable performance in proposed § 1033.311(c)(1) to implement the statutory requirement that covered data be made available in an electronic form usable by authorized third parties. This proposed requirement would carry out the objectives of CFPA section 1033 by ensuring that data providers make available data on a basis that enables third parties to provide products and services, including those that compete with products and services offered by the data provider.

Quantitative Minimum Performance Specification (§ 1033.311(c)(1)(i))

The current performance of data providers' developer interfaces is not always adequate, and whether a developer interface's performance is commercially reasonable cannot only be based on the performance of a data provider's peers. Thus, the CFPB has preliminarily determined that it is necessary to propose a firm quantitative floor to ensure that the performance improves in the near term.

The quantitative minimum performance specification in proposed § 1033.331(c)(1)(i) would be a response rate of at least 99.5 percent. That is, the CFPB proposes that the performance of a developer interface cannot be commercially reasonable unless the interface has a response rate (defined below) of at least 99.5 percent. The CFPB has preliminarily determined that this level of response rate would be an appropriate floor for commercially reasonable performance for several reasons. The CFPB understands from the Provider Collection that a number of data providers' extant consumer interfaces generally meet or exceed this level of performance. Further, the level of performance data providers can achieve with their consumer interfaces, in which the amount and variety of data are generally broader than the set of data the CFPB proposes to define as covered data, suggests this level of performance should be achievable for developer interfaces. In general, ensuring parity between consumer interfaces and developer interfaces will ensure that data providers make available data in a manner that is usable to consumers. In addition, Australia and the United Kingdom set their thresholds at 99.5 percent.[76] Their thresholds are calibrated from existing endpoints of data providers in both countries and suggest that data providers generally are able to meet a 99.5 percent threshold.[77] Moreover, the substantial preponderance of the respondents to the Provider Collection meet or exceed that level of performance. Thus, the CFPB has preliminarily determined that data provider interfaces cannot perform to commercially reasonable standards below a quantitative minimum performance specification of 99.5 percent. The CFPB requests comment specifically on what role qualified industry standards should have, if any, regarding the quantitative minimum performance specification set forth in the final rule.

Defining Proper Response Rate

The CFPB proposes to specify in § 1033.311(c)(1)(i) how the proper response rate would be calculated within a given time period, such as a month: that rate would be the number of proper responses by the interface divided by the total number of queries to the interface.

A proper response would be a response, other than an error message during unscheduled downtime, that meets the following three criteria: (1) the response either fulfills the query or explains why the query was not fulfilled; (2) the response complies with the requirements of proposed part 1033; and (3) the response is provided by the interface within a commercially reasonable amount of time. With respect to the third criterion, the CFPB proposes that the amount of time cannot be commercially reasonable if it is more than 3,500 milliseconds. It is possible under the CFPB's proposed rule that the amount of time for the response would not be commercially reasonable even if it were less than 3,500 milliseconds. The CFPB requests comment on whether any generally applicable industry standard sets forth an amount of time that should be used in lieu of 3,500 milliseconds.

The CFPB proposes that any responses by and queries to the interface during scheduled downtime for the interface would be excluded from the calculation of the proper response rate. Further, the CFPB proposes that any downtime of the interface would qualify as scheduled downtime only if the data provider has provided reasonable notice of the downtime to all third parties to which the data provider has granted access to the interface. The CFPB also proposes that the total amount of scheduled downtime for the interface must be reasonable. Adherence to a qualified industry standard would be an indication that the notice of downtime and the total amount of downtime are reasonable. The CFPB requests comment on whether it should provide additional detail on the amount of scheduled downtime that would constitute a reasonable amount. The CFPB also requests comment on whether it should provide additional detail on when and how a data provider must provide notice of scheduled downtime to third parties for the notice to be reasonable. For example, the Australia Consumer Data Standards state that normal planned outages should be reported to third parties with at least one week of lead time, and the UK Open Banking Standards provide that notice for planned downtime should be given at least five business days in advance.[78]

[76] Australia Consumer Data Standards, *Availability Requirements, https://consumerdatastandardsaustralia.github.io/standards/#availability-requirements* (last visited Sept. 16, 2023); Open Banking Ltd., *Operational Guidelines—Availability, https://standards.openbanking.org.uk/operational-guidelines/availability-and-performance/key-indicators-for-availability-and-performance-availability/latest/* (last visited Sept. 16, 2023).

[77] In the period from July 2022 to July 2023, UK account providers had an average weighted Open Banking API availability of 99.66 percent. *See* Open Banking Ltd., *API Performance Stats, https://www.openbanking.org.uk/api-performance/* (last visited Sept. 16, 2023). From December 1, 2021, through September 1, 2023, Australian data holders maintained a platform availability of 96.28 percent. *See* Australian Consumer Data Right, *Performance, https://www.cdr.gov.au/performance* (last visited Sept. 16, 2023).

[78] *See* Consumer Data Standards, *Availability Requirements, https://consumerdatastandards australia.github.io/standards/#session-requirements* (last visited Oct. 2, 2023); Open Banking Ltd., *Change and Communication Management—Downtime, https://standards.openbanking.org.uk/*

Indicia of Commercially Reasonable Performance (§ 1033.311(c)(1)(ii))

Proposed § 1033.311(c)(1) would require that the performance of a data provider's developer interface be commercially reasonable. While satisfaction of the quantitative minimum of 99.5 percent in proposed § 1033.311(c)(1)(i) would be necessary for commercially reasonable performance, it would not be sufficient. That is, under the CFPB's proposed rule it is possible that the performance of a data provider's developer interface would not be commercially reasonable notwithstanding that it does satisfy the quantitative minimum.

To provide a regulatory mechanism and incentive through which the performance of data providers' developer interfaces would improve in the future beyond the quantitative minimum, the CFPB is proposing, in addition to that minimum, two indicia of commercially reasonable performance in § 1033.311(c)(1)(ii) that can be expected to evolve over time. The first would be whether the performance of the interface meets the applicable performance specifications set forth in a qualified industry standard, as defined in proposed § 1033.131. The CFPB has preliminarily determined that the recurring process of developing, adopting, and revising a standard that is a qualified industry standard under the CFPB's proposed definition of that term would be probative of whether performance of the developer interface is commercially reasonable because it would take into account the interests of a wide variety of stakeholders, as discussed more fully in proposed § 1033.141.

The second would be whether the performance meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers. As the performance of similarly situated data providers' interfaces improves, the performance of a given data provider's developer interface also would have to improve to continue to meet this indicator of commercial reasonability. Conversely, as the performance of the given data provider's developer interface improves, that improvement would lead other similarly situated data providers to improve the performance of their interfaces to meet the performance of the given data provider.

The CFPB requests comment on whether additional indicia would be appropriate and what they should be. Currently, agreements and standards name and describe specifications, such as latency and uptime, for the performance of data providers' developer interfaces. The CFPB requests comment on whether the final rule, instead of referring broadly to ''applicable performance specifications,'' should name and describe certain specifications. For example, rather than providing that indicia of compliance include meeting the applicable performance specifications achieved by the developer interfaces of similarly situated data providers, the final rule could provide that indicia include meeting the latency and uptime specifications achieved by the interfaces of the other data providers.

The CFPB also notes that each data provider would have some information about the performance of other data providers' interfaces because (as discussed below) the CFPB is proposing in § 1033.341(c) to require all data providers to disclose publicly the quantitative proper response metric for their developer interfaces. The CFPB also seeks comment on what sources of market information data providers would use to evaluate the performance of their peers' developer interfaces.

Access Cap Prohibition for Data Providers' Interfaces (§ 1033.311(c)(2))

The CFPB proposes 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 the data provider's developer interface. Such restrictions are commonly known as ''access caps'' or ''rate limits.'' CFPA section 1033(a) requires that data providers make available covered data upon request. The CFPB has preliminarily determined that this proposed provision would be necessary and appropriate to effectuate consumers' statutory rights under CFPA section 1033 by ensuring that consumers and their authorized third parties are not impeded from exercising consumers' statutory rights, including through unreasonably frequent data requests by other authorized third parties.

Under proposed § 1033.311(c)(2), a data provider would be prohibited from unreasonably restricting the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface, except as set forth in certain sections. Those sections are proposed § 1033.221, which restates the statutory exceptions in CFPA section 1033(b); proposed § 1033.321, which describes the risk management reasons applicable to denying a third party's access to an interface; proposed § 1033.331(b), which identifies the conditions for when a data provider must respond to an information request; and proposed § 1033.331(c), which identifies other reasons a response would not be required.

The CFPB does not intend that proposed § 1033.311(c)(2) would allow a data provider to impose restrictions that would override a consumer's authorization, including the frequency with which an authorized third party requests data. Instead, the proposed provision would allow restrictions only if they reasonably target a limited set of circumstances in which a third party requests information in a manner that poses an unreasonable burden on the data provider's developer interface and impacts the interface's availability to other authorized third party requests. To prevent abuse of this provision, proposed § 1033.311(c)(2) provides that 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 pursuant to proposed § 1033.351(a). Indicia that any frequency restrictions applied are reasonable would include that they adhere to a qualified industry standard.

The CFPB proposes in § 1033.311(c)(2) to prohibit unreasonable access caps for developer interfaces pursuant to both its authority under CFPA sections 1033(a) and 1022(b)(1). A data provider that imposes an access cap for which it has no reasonable basis would not be making available covered data upon request by authorized third parties. Prohibiting unreasonable access caps would ensure consumers and third parties are not impeded from exercising consumers' rights under the statute based on unreasonable limits imposed by the data provider.

The CFPB requests comment on whether the proposed provision should be defined more narrowly to prevent data providers from interfering with a consumer's authorization or whether additional guidance is needed to prevent abuse. For example, the CFPB requests comment on whether the final rule should include a presumption that access caps are unreasonable unless undertaken for a period only as long as necessary to ensure a third party request does not interfere with the receipt of and response to requests from other third parties accessing the interface.

operational-guidelines/change-and-communication-management/downtime/latest/ (last visited Oct. 2, 2023).

The CFPB also requests comment on whether data providers should be permitted to restrict the total amount of covered data that third parties request over a given period of time and on whether proposed part 1033 should treat small versus large data providers differently in this regard. The CFPB also requests comment on whether there should be different restrictions on data providers' access caps in cases where the consumer is actively online with a third party requesting data access, as opposed to when data are being automatically refreshed without a consumer present.

Security Specifications (§ 1033.311(d))

The CFPB is proposing to require data providers to implement several data security features in their consumer and developer interfaces. This provision would implement CFPA section 1033(a) by clarifying how a data provider would ensure it is making data available to a consumer, including an authorized third party, in a manner that would carry out the objectives of CFPA section 1033. Certain provisions also would promote the use and development of standardized formats, consistent with CFPA section 1033(d).

Access Credentials

As discussed throughout part I, third parties' credential handling practices—typically resulting from their reliance on credential-based screen scraping—can raise significant security, risk management, privacy, and accuracy risks to the system as a whole. Proposed § 1033.311(d)(1) would seek to prevent data providers from relying on a third party's use of consumer credentials to access the developer interface.

When they employ screen scraping, third parties generally must store consumer account credentials they obtain so they can be reused to collect data as necessary to support the product or service a consumer is using. Because third parties collect data from many consumers at once, they must collect and store many sets of consumer credentials. This creates security and fraud risks: bad actors might target third parties and attempt to cause a data breach because these third parties store large quantities of sensitive consumer information. The longer a third party stores consumer credentials before deleting them, and the less rigorous a third party is in employing cybersecurity practices to protect those credentials, the more likely such a breach will occur. If a breach occurs—whether because of inadequate cybersecurity or credential storage practices, or for any other reason—the consumers to whom the leaked credentials correspond may suffer invasions of privacy or financial harms. This is especially the case for the kinds of funds-storing and payment accounts that would be covered by this proposed rule; a breach which results in the theft of credentials could cause unauthorized transactions or fraudulent use of consumers' personal financial data. For data providers, designing developer interfaces that operate using consumers' access credentials would heighten the risks described in part I.C and create specific risks to data providers. For example, a data provider may face greater difficulty ensuring legitimate access by third parties using a consumer's credentials, impairing its efforts to prevent truly unauthorized access by criminals or other bad actors. The widespread use of consumers' access credentials in a developer interface could also raise risk management concerns.[79]

To avoid these problems from arising because of how a data provider's developer interface is designed, proposed § 1033.311(d)(1) would prohibit a data provider from allowing a third party to access the data provider's interface by using any credentials that a consumer uses to access the consumer interface.

The CFPB understands that in current arrangements between data providers and third parties for use of data providers' developer interfaces, the data provider often authenticates the consumer using that consumer's digital banking credentials. In such cases, the CFPB understands that the third party itself does not request, access, use, or retain the consumer's credentials; instead, after procuring a consumer's authority to access data, the third party 'passes' the consumer directly to the data provider, who authenticates the consumer using the consumer's digital banking credentials, and then provides the third party with a secure access token. The CFPB seeks comment on whether and, if so, how the proposed rule should address this practice.

The CFPB also understands that, in some cases, entities that act as service providers to data providers may develop, deploy, and maintain developer interfaces on behalf of those data providers whose technical specifications and requirements entail those service providers retaining and using consumers' credentials. Such arrangements can provide lower-cost routes for smaller data providers to offer developer interfaces, which benefits all participants in the open banking system and, ultimately, consumers. The CFPB does not intend for proposed § 1033.311(d)(1) to interfere with such arrangements but seeks comment on situations where an entity acts as both such a service provider and a third party.

Security Program

Proposed § 1033.311(d)(2) would address general data security requirements for the data provider's developer interface. Because the proposed definition of covered data includes transaction information, information for initiating payments to or from a consumer's account, and other sensitive financial information, poor data security measures would expose consumers to significant harm, such as fraud or identity theft. As the CFPB noted in a recent circular, information security weaknesses can result in data breaches, cyberattacks, exploits, ransomware attacks, and other exposure of consumer data.[80] To prevent these harms, the proposed rule would require data providers to apply to their developer interfaces a data security program that satisfies the GLBA Safeguards Framework. The proposed rule would require a data provider that is not a GLBA financial institution to apply the information security program required by the FTC's Safeguards Rule.[81]

The CFPB has preliminarily determined that the GLBA Safeguards Framework appropriately addresses data security risks for developer interfaces in the market for consumer-authorized financial data. 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 rule. The 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. This flexible,

[79] *See generally* Fed. Rsrv. Sys., FDIC, OCC, *Interagency Guidance on Third-Party Relationships: Risk Management* (June 6, 2023), *https://occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf.*

[80] Consumer Fin. Prot. Bureau, *Consumer Financial Protection Circular 2022–04* (Aug. 11, 2022), *https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.*

[81] 16 CFR part 314.

risk-based approach allows it to adapt to changing technology and emerging data security threats.

Requiring data providers to apply the GLBA Safeguards Framework would also reduce burden by avoiding duplicative or inconsistent data security requirements. The CFPB understands that all or nearly all data providers are already subject to the GLBA Safeguards Framework, and therefore would be able to adapt their information security programs to the risks created by the developer interface. For example, a State member bank would apply the information security program that it had developed pursuant to the Interagency Guidelines Establishing Information Security Standards issued by the Board of Governors of the Federal Reserve System.[82]

The CFPB considered proposing to require data providers to adopt additional reasonable policies and procedures regarding the data security of the interfaces for third parties. Such a requirement would share the GLBA Safeguards Framework's flexibility to accommodate changing technology and emerging threats while avoiding the potential uncertainty of applying the GLBA Safeguards Framework's existing requirements to the open banking system. But a general policies and procedures requirement would lack the additional detail of the GLBA Safeguards Framework. Data providers already face a general obligation to avoid inadequate data security measures under the CFPA's prohibition on unfair, deceptive, and abusive acts and practices.[83] Supplying additional detail to a general policies and procedures requirement has several potential drawbacks. For example, the CFPB may end up adopting substantially similar requirements to the GLBA Safeguards Framework, thus subjecting data providers to duplicative data security regulations. Or the CFPB might adopt additional clarifications that are inconsistent with the Federal functional regulators' interpretation of the GLBA Safeguards Framework. For these reasons, the CFPB declines to propose a general policies-and-procedures requirement for data security but seeks comment on such a requirement.

Although the CFPB understands that the data security of data providers' interfaces for third parties is generally regulated by existing law, the proposed definition of data provider is broad enough to encompass a diverse array of entities. While the CFPB understands that all or virtually all data providers are GLBA-covered financial institutions, the proposed rule would remove any uncertainty by making compliance with the GLBA Safeguards Framework a requirement for any developer interface. For data providers not subject to the Interagency Guidelines issued by the Federal functional regulators,[84] the proposed rule would require compliance with the FTC's Safeguards Rule. As the FTC explained in its recent amendments to the Safeguards Rule, the Safeguards Rule is designed to operate without the benefit of direct guidance by an examining agency.[85] For this reason, the CFPB has preliminarily determined that the FTC's Safeguards Rule is appropriate for data providers that might not have the direct supervision of one of the Federal functional regulators that implement the Interagency Guidelines.

This proposed rule would implement CFPA section 1033(a) by clarifying how a data provider must make available data upon request to a consumer, which would include an authorized third party. Establishing a consistent set of data security requirements to developer interfaces 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)

Proposed § 1033.321 would 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). In particular, a data provider would not be required to make available covered data to a person or entity that presents significant risks to the data provider's data security or risk management program. 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.

Risk Management (§ 1033.321(a) Through (c))

The CFPB recognizes that data providers have legitimate interests in making data available only to authenticated consumers and authenticated authorized third parties and in a way that avoids unreasonable risks to consumers and protects covered data. CFPA section 1033(a) does not expressly address how a data provider must take risk management concerns into account when making data available. However, as discussed in this section below, the CFPB has preliminarily determined that CFPA section 1033(a) authorizes procedures to clarify the circumstances under which a data provider must make available covered data upon request. The CFPB is proposing to clarify that a data provider can reasonably deny a consumer or third party access to an interface described in proposed § 1033.301(a) based on risk management concerns.

Depository institutions have legal obligations to operate in a safe and sound manner, and both depository and nondepository institutions have other security-related obligations.[86] The prudential regulators have issued guidance explaining that, to operate in a safe and sound manner, banking organizations must establish practices to manage the risks arising from third party relationships.[87] The guidance explains that ''[c]onducting due diligence on third parties before selecting and entering into third party relationships is an important part of sound risk management.'' [88] The guidance further explains that ''[n]ot all relationships present the same level of risk, and therefore not all relationships require the same level or type of oversight or risk management.'' [89] Additionally, data security guidelines issued by the prudential regulators and

[82] 12 CFR part 208, app. D–2.

[83] Consumer Fin. Prot. Bureau, *Consumer Financial Protection Circular 2022–04* (Aug. 11, 2022), *https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/*.

[84] *See* 12 CFR 1016.3(k) (defining ''Federal functional regulator'' as the Board of Governors of the Federal Reserve System, the OCC, the Board of Directors of the FDIC, the NCUA Board, and the Securities and Exchange Commission).

[85] 86 FR 70272, 70287 (Dec. 9, 2021).

[86] *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); the GLBA; the FTC's Safeguards Rule; Fed. Fin. Insts. Examination Council, *Authentication and Access to Financial Institution Services and Systems* (Aug. 11, 2021), *https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf* (Security Guidelines).

[87] Bd. of Governors of the Fed. Rsrv. Sys., Fed. Deposit Ins. Corp., Off. of the Comptroller of the Currency, Dep't of the Treas., *Interagency Guidance on Third-Party Relationships: Risk Management,* 88 FR 37920, 37927 (June 9, 2023) (Interagency TPRM Guidance).

[88] *Id.* at 37929.

[89] *Id.* at 37927.

the FTC also address risk management. For example, the prudential regulators' data security guidance states that banks should implement controls to identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information.[90]

The SBREFA Panel recommended that the CFPB clarify the circumstances under which data providers would be required to make data available to third parties.[91] The Panel also recommended that the CFPB evaluate options that would allow data providers to take reasonable steps to reduce security and fraud risks, while still ensuring that consumers are able to exercise their rights under the eventual rule.[92] Further, various stakeholders have asked the CFPB to clarify whether a data provider would violate the proposed rule if it were to deny access to a third party based on a legitimate risk management concern. The CFPB has developed proposed § 1033.321(a) through (c) to address this feedback.

Consumers could be harmed if a 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. For example, if a data provider had legitimate concerns about a third party's ability to safeguard the consumer's data, requiring that data provider to nevertheless grant access to the third party could result in a data breach that could have been avoided. At the same time, if denials of access are not narrowly tailored to a specific risk management concern, they may frustrate a consumer's right to access data under CFPA section 1033. As discussed in part I.C, the CFPB is concerned that data providers may have incentives to deny access, particularly where third parties are offering a competing product or service, which may result in denials that are not tailored to a legitimate risk.

To address this possibility, proposed § 1033.321(a) states that a data provider can reasonably deny a consumer or third party access to its interface based on risk management concerns, as clarified by proposed § 1033.321(b) and (c). Subject to proposed § 1033.321(b), discussed below, a denial would not be unreasonable if it is necessary to comply with the safety and soundness requirements or data security requirements in Federal law.

Proposed § 1033.321(b) explains that to be reasonable under proposed § 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 the third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner. The CFPB notes that the term ''non-discriminatory'' in this paragraph carries its ordinary meaning and is not intended to refer to discrimination on a prohibited basis under Federal fair lending law.[93] For example, if a denial were to be based on a concern about consumer-authorized data access generally, rather than a specific risk related to the operations or practices of the third party requesting data, it would not be reasonable. In addition, if a data provider were to deny access to one third party based on a certain risk but were to grant access to another third party where the same risk is present, and all other factors were equal, the denial would not be considered reasonable.

Proposed § 1033.321(c) explains that indicia that a denial is reasonable include whether access is denied pursuant to the terms of a qualified industry standard related to data security or third party risk management. If a data provider were to deny access to comply with these requirements, the denial may be reasonable because it reflects compliance with standards developed with the participation of a variety of stakeholders in the open banking system, consistent with the proposed rule's objective discussed in part I.D to develop a data access framework that is safe and competitive. However, conformance with an industry standard alone would not necessarily settle the question of reasonableness.

The CFPB requests 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. Risk management may entail a variety of practices and risk management standards could be defined through several sources, including prudential guidance, other Federal government standards, or qualified industry standards. The CFPB requests comment on the extent to which CFPB rule 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.

Proposed § 1033.321(a) through (c) would implement CFPA section 1033 by clarifying what steps are necessary to make data available to a consumer or authorized third party upon request. These provisions would seek to ensure that data providers are making data available only to authenticated consumers and authenticated authorized third parties, and that data access does not present unreasonable risks to the security and integrity of covered data. Depending on the facts, certain exceptions under CFPA section 1033, set forth in proposed § 1033.221, might allow a data provider to not make data available.[94] However, the CFPB has preliminarily determined that, in most cases, it would not be appropriate for data providers to rely on the exceptions to address risk management concerns. The identification of risk management concerns might involve the exercise of substantial discretion by the data provider, and the CFPB is concerned that data providers' strong competing incentives discussed in part I.C might undermine the objectives of CFPA section 1033 to allow consumers to share data with authorized third parties, in particular third parties offering competing products or services.

Denials Related to Lack of Information—Evidence of Data Security Practices (§ 1033.321(d)(1))

The CFPB is proposing that a data provider would have a reasonable basis for denying a third party access to a developer interface under proposed § 1033.321(a) if a third party does not present evidence that its data security practices are adequate to safeguard the covered data.

As noted in the discussion of proposed § 1033.321(a) through (c), data providers are subject to various legal obligations related to data security, and safety and soundness. Consistent with these obligations, data providers in the market today typically conduct due diligence of a third party before granting the third party access to the data provider's interface. This diligence is typically either performed by the data provider itself or by another entity, such as a data aggregator, a core banking provider, or a third party assessment firm.

[90] *See, e.g.,* Security Guidelines at III.B.1.

[91] SBREFA Panel Report at 44.

[92] *Id.*

[93] A similar requirement is found in the information blocking provision of HHS's rule implementing the 21st Century Cures Act, Public Law 114–255, 130 Stat. 1033 (2016). *See* 85 FR 25642, 25862 (May 1, 2020).

[94] *See, e.g.,* 12 U.S.C. 5533(b)(2) (exception for any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct), 5533(b)(3) (exception for any information required to be kept confidential by any other provision of law).

If the CFPB finalizes the rule as proposed, data providers that currently have developer interfaces could experience an increased volume of requests. In addition, some data providers will be establishing interfaces for the first time. The CFPB is concerned that, particularly for smaller data providers, the volume of requests from third parties to access these data providers' interfaces could outstrip these data providers' resources for vetting third parties. In addition to being burdensome for individual data providers, the CFPB is also concerned that duplicative vetting—*i.e.,* several different data providers conducting similar due diligence of a particular third party—could be a source of inefficiency in the open banking system.

In some other open banking regimes, a governmental or quasi-governmental body addresses these potential problems by serving an accreditation function. The governmental or quasi-governmental body independently evaluates third parties and issues credentials endorsing the third party's fitness to receive consumer-authorized data.[95] The CFPB is proposing a different approach to standard-setting. Although a private accreditation system does not yet exist in the United States, there are various certifications in existence today that represent compliance with certain data security standards.

Proposed § 1033.321(d)(1) would seek to alleviate the concerns described above related to the potential burden of vetting on smaller data providers and the potential inefficiency resulting from duplicative vetting. Proposed § 1033.321(d)(1) states that a data provider has a reasonable basis for denying access to a third party under proposed § 1033.321(a) if the third party does not present evidence that its data security practices are adequate to safeguard the covered data. Where the third party does not present such evidence, the data provider may deny access under proposed § 1033.321(a) without vetting the third party. Where the third party does present such evidence, the data provider may either grant access or perform additional due diligence on the third party as appropriate.

The CFPB requests 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 under proposed § 1033.321(d)(1), and what types of evidence might provide such a basis. For example, the CFPB requests comment on whether such evidence could consist of certifications or other credentials representing compliance with data security standards, or evidence of vetting by a third party risk assessment firm.

As the text of proposed § 1033.321(d)(1) explains, any denials of access under this provision would still be subject to the reasonability requirement in proposed § 1033.321(a). For example, proposed § 1033.321(b) states in part that, to be reasonable, a denial on risk management grounds must be applied in a consistent and non-discriminatory manner. Thus, a data provider could not deny access to a third party for failing to present evidence that its data security practices are adequate to safeguard the covered data, where it grants access to another third party that presents similar evidence, assuming all other factors are equal.

The CFPB encourages stakeholders in the open banking system to engage in a fair, open, and inclusive process to develop an accreditation system for third parties. For example, data providers, third parties, consumer advocacy groups, and other stakeholders could establish an independent body that performs an accreditation role, or an existing open banking standards body could expand its remit to include such a role. The CFPB requests comment on whether developing such a credential could reduce diligence costs for both data providers and third parties and increase compliance certainty for data providers with respect to the proposed rule. The CFPB also requests comment on the steps necessary to develop such a credential and how the CFPB or other regulators could support such efforts.

Denials Related to Lack of Information—Certain Information About the Third Party (§ 1033.321(d)(2))

The CFPB is proposing that a data provider would have a reasonable basis for denying access under proposed § 1033.321(a) if a third party does not make public certain information about itself. The CFPB has preliminarily determined that this provision would enable the open banking system to function more efficiently, in two respects.

First, the information would help data providers authenticate the identities of third parties (*i.e.,* help data providers confirm the third party is who they say they are). After a data provider establishes an interface, it may receive a request from a third party to access that interface, but it may not know who the third party is. The identity information described in proposed § 1033.321(d)(2)(i) through (iii)—the third party's legal name and any assumed name they are using when doing business with the consumer, a link to their website, and their LEI—would help the data provider confirm the third party's identity. Second, the information described in proposed § 1033.321(d)(2)(iv)—contact information a data provider can use to inquire about the third party's data security practices—would facilitate any outreach to the third party that may be required as part of a data provider's diligence. Furthermore, the identity information described in proposed § 1033.321(d)(2)(i) through (iii) may help the data provider conduct research in connection with its due diligence.

The SBREFA Panel recommended that the CFPB evaluate options that would reduce additional costs on data providers and third parties in authenticating a third party or verifying a third party's authorization, such as providing data providers with a list of third parties that make available information relevant to their authentication.[96] By assisting data providers with third party authentication and due diligence, the CFPB has preliminarily determined that proposed § 1033.321(d)(2) would help further the recommendations of the SBREFA Panel related to third party authentication.[97]

Proposed § 1033.321(d)(2) would permit the data provider to deny access if the information is not available in human-readable and machine-readable formats. Making the data available in machine-readable format could enable data providers and other stakeholders to use automated processes to ingest the relevant information into their systems for processing and review, which would make the process of obtaining this information more efficient. Proposed § 1033.321(d)(2) would also permit the data provider to deny access 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 seeks 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.

[95] *See, e.g.,* Australian Gov't, *Become an Accredited Data Recipient, https://www.cdr.gov.au/for-providers/become-accredited-data-recipient* (noting that the Australian Competition and Consumer Commission ''manages the accreditation process'') (last visited Aug. 19, 2023).

[96] SBREFA Panel Report at 44.

[97] *Id.* at 43.

The CFPB seeks comment on 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. For example, the CFPB could provide that a data provider is permitted to deny access if the third party's information is not available on public websites and the URL does not contain specified text in accordance with the ''well-known Uniform Resource Identifier'' protocol. This approach could make it easy for a person to identify the website where a particular third party's information is available or all websites where third parties are making such information available, which could facilitate the creation of a directory of third parties.

Additionally, the CFPB seeks comment on 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. This would enable the CFPB to publish a directory of links that data providers and other members of the public could use. The CFPB also seeks comment on 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. For example, data providers could be required to regularly provide the CFPB a list of all third parties that they have approved to access their interface. As a further example, data providers could be required to notify the CFPB if and when they deny a third party access to their developer interface, including reasons for denying access (records of which proposed § 1033.351(d)(2)(i) would require data providers to retain). Such information may allow the CFPB to better monitor the data access system and ensure that denials of access are compliant.

Under proposed § 1033.321(d)(2), the information the third party makes available would be disclosed publicly. Public disclosure of this information—along with public disclosure of similar information by data providers pursuant to proposed § 1033.341—would facilitate market monitoring by the CFPB and members of the public. It would also enable standard-setting bodies to identify the data providers and third parties that are participating in the open banking system, which could aid efforts by standard-setting bodies to develop industry standards related to consumer-authorized data access.

The CFPB proposes in § 1033.321(d)(2) that a data provider would have a reasonable basis for denying a third party's access to covered data in certain situations pursuant to the CFPB's authority under CFPA sections 1033(a) and 1022(b)(1). By requiring a third party to make public certain identifying information about itself, the disclosures proposed in § 1033.321(d)(2) serve as a component of the statutory requirement of CFPA section 1033(a) to make data available. The disclosures facilitate CFPA section 1033's data availability requirement by giving data providers an authentication tool over third parties, while also facilitating any outreach required by data providers to a third party as a result of the data provider's due diligence obligations under proposed § 1033.321(a) through (c). Additionally, these disclosures would be authorized under CFPA section 1022(b)(1), which authorizes the CFPB to prescribe rules as may be necessary or appropriate to enable the CFPB to prevent evasion of the purposes and objectives of the Federal consumer financial laws—including carrying out the objectives of CFPA section 1033.

The SBREFA Panel recommended that the CFPB consult with other Federal agencies responsible for administering data security requirements applicable to data providers to discuss the feasibility of developing a safe harbor for authenticating third parties.[98] Due to the lack of an accreditation system in the United States related to open banking—as described above in the discussion of proposed § 1033.321(d)(1)—the CFPB has preliminarily determined that such a safe harbor for the proposed rule is not feasible at this time. The CFPB plans to engage in further coordination with the Federal agencies responsible for administering data security requirements.

While the CFPB is not proposing a safe harbor, proposed § 1033.321(a) through (c) would seek to reduce a data provider's uncertainty about when they may deny access to an interface based on risk management concerns. Further, proposed § 1033.321(d)(1) and (2) would seek to alleviate the potential burden of vetting on data providers. Last, proposed § 1033.321(d)(2) would help data providers authenticate the identities of third parties. The CFPB seeks comment on how the proposed rule could further facilitate compliance and reduce due diligence costs for both data providers and third parties while adequately ensuring the security of consumer data.

[98] *Id.* at 44.

5. Responding to Requests for Information (§ 1033.331)

Proposed § 1033.331 would prescribe basic conditions to implement data providers' obligation to make data available ''upon request'' under CFPA section 1033(a) and would clarify data providers' ability to authenticate and manage the authorization process for third parties. In general, under proposed § 1033.331, a data provider would need to make covered data available to the third party in accordance with the terms of the authorization provided by the consumer to the third party if the conditions in proposed § 1033.331(b) were satisfied, as discussed below. A data provider would not be required to make data available if one of the exceptions listed in proposed § 1033.221 applied, if the data provider reasonably denied access pursuant to proposed § 1033.321(a), if the data provider's interface were unavailable, or if a third party's authorization was no longer valid.

Responding to Requests—Access by Consumers (§ 1033.331(a))

Proposed § 1033.331(a) would prescribe the conditions that apply where consumers are seeking covered data (as opposed to where a third party requests access to a consumer's data on the consumer's behalf). Under proposed § 1033.331(a), a data provider would be required to make available covered data upon request to a consumer when it receives information sufficient to (1) authenticate the consumer's identity and (2) identify the scope of the data requested. Under proposed § 1033.331(a), the CFPB expects that these conditions would be satisfied through procedures in use by most consumer interfaces that automatically authenticate consumers and allow consumers to identify covered data.

Responding to Requests—Access by Third Parties (§ 1033.331(b))

Proposed § 1033.331(b)(1) would list four conditions that must be satisfied to clarify when a data provider must make available covered data to a requesting third party acting on behalf of a consumer. Under proposed § 1033.331(b)(2), data providers would be permitted to engage in limited steps to confirm conditions are satisfied with respect to a third party's authorization.

Stakeholders have expressed different views about whether and the extent to which data providers, third parties, or both, should manage the process of obtaining a consumer's authorization to grant a third party access to the

consumer's data.[99] In response to the SBREFA Outline, the CFPB received feedback from several stakeholders expressing concern that reliance on an authorization generated by a third party would present risk management concerns and that they should be able to obtain the consumer's authorization from the consumer. Stakeholders have also suggested that this approach is necessary to protect consumer privacy and data security. Other stakeholders have suggested that the data provider should be able to confirm the consumer's authorization before making data available to the third party.[100]

As discussed in part III, the CFPB interprets CFPA section 1033 to authorize rules that require data providers upon request to readily make available usable data to consumers and authorized third parties, including third parties offering competing products and services. The CFPB has preliminarily determined that third parties are in the best position to determine what covered data are reasonably necessary to provide the requested product or service. And as discussed in part I.C, data providers may have strong incentives to limit the scope of data available to third parties, especially those providing a competing product or service.

The CFPB recognizes that data providers have legitimate interests in protecting their data security and other risk management priorities. Accordingly, the CFPB has preliminarily determined that data providers should confirm the third party's authorization with the consumer, as discussed below with respect to proposed § 1033.331(b)(2), as well as other provisions designed to protect legitimate security and other risk management interests, such as those discussed with respect to proposed § 1033.321. While the CFPB is proposing to allow data providers to reasonably deny access requests due to a risk management concern described in proposed § 1033.321(a), the CFPB does not intend for data providers to rely on this provision to limit the scope of a consumer's authorization. Proposed § 1033.321(a) would only allow a data provider to deny a third party access entirely to its developer interface, and a data provider likely would not have a reasonable basis to deny a third party access to an interface entirely due to concerns specifically about the scope of data requested.

The CFPB also acknowledges third parties may present security and privacy risks to consumers, as discussed in part I.C. However, the CFPB is proposing procedures discussed in part IV.D to ensure third parties are acting on behalf of consumers. The CFPB does not believe primary enforcement responsibility for ensuring third parties are acting on behalf of consumers should reside with data providers that may be driven by their own commercial interests. For the reasons above, the CFPB has preliminarily determined that it would best carry out the objectives of CFPA section 1033 for data providers to confirm that the third party has followed the authorization procedures described further below with respect to proposed § 1033.401. These procedures are discussed in greater detail below with respect to proposed § 1033.331(b)(1)(iii).

Conditions That Apply to Requests From Third Parties (§ 1033.331(b)(1))

Among the four conditions that would trigger a response to a third party under proposed § 1033(b)(1), a data provider would need to receive information sufficient to authenticate the consumer's identity. The CFPB is proposing to include this condition to mitigate the potential for fraudulent data requests.[101] In the market today, before a data provider grants a third party access to covered data, the consumer is typically redirected 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). The CFPB seeks 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.

In addition to authenticating the consumer's identity, under proposed § 1033.331(b)(1)(ii), the data provider would need to receive information sufficient to authenticate the third party's identity. 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. As discussed with respect to proposed § 1033.321(a), the proposed rule would not require data providers to make data available to third parties that present legitimate risk management concerns. The CFPB expects that, prior to responding to data requests, most data providers would engage in some reasonable risk management diligence in accordance with proposed § 1033.321(a) as part of approving third parties to access a developer interface. And as discussed below with respect to proposed § 1033.331(c)(2), a data provider would not need to respond to a request from a third party if the data provider has a proper basis to deny access pursuant to risk management concerns described in proposed § 1033.321(a).

Further, 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, discussed in greater detail in part IV.D. 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. The CFPB requests 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, under proposed § 1033.331(b)(1)(iv), a data provider would need to receive information sufficient to identify the scope of the data requested. Under proposed § 1033.301(a), in response to a request (that satisfies the conditions of proposed § 1033.331(b)(1)), a data provider would be required to make available the requested covered data. In some circumstances, however, the scope of information requested by an authorized third party might be ambiguous. To clarify the scope of covered data to be made available in response to a request, a data provider could seek to clarify the scope of an authorized third party's request with a consumer. For example, 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 requests 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

[99] *See, e.g., id.* at 30.

[100] *See, e.g., id.* at 54.

[101] This can include cases where the initial query under a request is being given by a fraudster or another person not actually authorized by the consumer, or cases where queries pursuant to an earlier-given authorization are pursuant to the actions of a fraudster or other unauthorized party that has illicitly gained control of a consumer's account or identity.

forth in proposed § 1033.331(b)(1) in a way that frustrates the ability of authorized third parties to receive timely responses to requests for covered data.

Confirmation of Third Party Authorization (§ 1033.331(b)(2))

Proposed § 1033.331(b)(2) provides that a data provider is permitted to confirm the scope of the 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 that will be accessed, by presenting that information—as it is disclosed on the authorization disclosure—back to the consumer. This confirmation step would enable the data provider to confirm the account(s) to which the third party is seeking access, which may not be clear from the authorization disclosure. For example, a consumer might have multiple accounts with a data provider, and it may be unclear from the authorization disclosure which account (or accounts) the request pertains to, because the third party would not necessarily know the names and account numbers of the consumer's accounts. This step also would give the consumer an opportunity to review information about what data they would be authorizing the third party to access, and it would give data providers greater certainty that the consumer has authorized the request. The CFPB seeks comment on whether the final rule should instead permit data providers to confirm this information with the consumer only where reasonably necessary. Under this alternative approach, if technology were to evolve such that data providers could reasonably confirm this information without asking the consumer to confirm it, the rule might no longer permit data providers to ask consumers to confirm this information.

Response Not Required (§ 1033.331(c))

Proposed § 1033.331(c) would list the four circumstances under which a data provider would not be required to make covered data available in response to a request. For ease of reference, proposed § 1033.331(c)(1) and (2) would restate exceptions that exist elsewhere in the proposed rule: the exceptions in proposed § 1033.221, which are derived from section 1033(b) of the CFPA, and the exception in proposed § 1033.321(a) related to risk management.

Proposed § 1033.331(c)(3) explains that a data provider would not be required to make covered data available if its interface is not available when the data provider receives a request. Under proposed § 1033.331(c)(3), if a data provider receives a request, and the data provider's interface is unavailable, the data provider would not violate its obligation to make covered data available where it does not respond to the request. Proposed § 1033.331(c)(3) explains, however, that the data provider would be subject to the performance specifications in proposed § 1033.311(c). The CFPB requests comment on any additional clarification that would reduce the opportunity for data providers to deny requests without justification under this provision. For example, the CFPB could clarify the meaning of ''unavailable'' in a manner similar to the ''infeasibility'' or ''health IT'' exceptions in the Information Blocking Rule issued by HHS.[102]

Finally, proposed § 1033.331(c)(4) explains that a data provider would not be required to make covered data available 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).

Jointly Held Accounts (§ 1033.331(d))

The CFPB is proposing to identify a data provider's obligation to make covered data available upon request where a consumer jointly holds an account. Proposed § 1033.331(d) would 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 provide covered data to that consumer or authorized third party. This provision would not affect data providers' existing obligations to provide information directly to consumers under other Federal consumer financial laws, such as EFTA, the Truth in Savings Act (TISA),[103] 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.[104] The CFPB seeks 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 seeks 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.

Data Provider Revocation (§ 1033.331(e))

The CFPB is proposing to permit a data provider to make available to the consumer a reasonable method by which the consumer may revoke any third party's authorization to access all of the consumer's covered data. Under proposed § 1033.331(e), to be reasonable, the revocation method must, at a minimum, 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. Indicia that the data provider's revocation method is reasonable would include its conformance to a qualified industry standard. Finally, a data provider that receives a revocation request from consumers through a revocation method it makes available must notify the authorized third party of the request.

This proposed provision—along with proposed § 1033.421(h), under which third parties must make available to consumers a mechanism by which consumers may revoke third party authorization—is intended to ensure consumers have multiple outlets and methods by which they may revoke third party authorization to access their data. The CFPB has preliminarily determined that requiring data providers to make available a revocation method may create a burden on smaller entities. The CFPB seeks to balance these competing considerations through a proposed rule that allows, but does not require, data providers to make available a revocation method.

The SBREFA Panel recommended the CFPB consider options that would allow consumers to revoke third party authorizations through both the third party and data providers.[105] The SBREFA Panel also recommended the CFPB continue to consider how revocation requirements could be designed to reduce impacts on third parties and data providers.[106]

Additionally, various stakeholders expressed concerns about anticompetitive activities related to data providers making a revocation method

[102] *See* 45 CFR 171.204; 171.205.

[103] 12 U.S.C. 4301 *et seq.*

[104] *See* 12 CFR 1005.4(c), 1030.3(d), 1026.5(d).

[105] SBREFA Panel Report at 44.

[106] *Id.* at 45.

available to consumers. As such, proposed § 1033.331(e) would permit data providers to make available a method for revoking a third party's access to ''all of the consumer's covered data.'' Proposed § 1033.331(e) would not permit a data provider to make available a method through which the consumer could partially revoke a third party's access to the consumer's data, *i.e.,* revoke access to some of the data the consumer had authorized the third party to access, but not other data it had authorized under the terms of the same authorization. For example, if the consumer consented in the initial authorization to share their deposit account and credit card data with a third party, the data provider could not make available a revocation method through which the consumer could revoke access to the deposit account but not the credit card account. Such a revocation method would be inconsistent with proposed § 1033.201(a), which would require data providers to make covered data available upon request based on the terms of the consumer's authorization. In addition, consumers who partially revoke access to their data could unintentionally disrupt the utility of data access for certain use cases.

To further account for anticompetitive concerns related to data providers making available a revocation method, proposed § 1033.331(e) includes a list of non-exhaustive requirements to ensure the optional revocation method is reasonable, including the extent to which it is 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. As noted in part IV.B.2, this language is drawn from the definition of ''information blocking'' set forth in section 3022(a) of the Public Health Service Act.[107] The CFPB preliminarily has determined that this language would promote consumers' ability to access and share their data by ensuring data providers do not impose obstacles that evade their obligations to make available covered data under section 1033.

Proposed § 1033.331(e) also states that one indication that a data provider's revocation method is reasonable is that it adheres to a qualified industry standard. The CFPB seeks comment on whether the final rule should impose any additional requirements to ensure the optional revocation method is reasonable and does not result in anticompetitive outcomes. The CFPB also seeks comment on types of conduct that could interfere with, prevent, or materially discourage access to or use of data, and whether the CFPB would need to provide guidance related to that conduct.

The CFPB is also proposing to require a data provider that receives a revocation request from a consumer to notify the authorized third party of the request. 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 permitted reason. The CFPB seeks comment on the implementation of this notification requirement, including, in cases where an authorized third party uses a data aggregator to access the authorized third party's access, to which party or parties the data provider must provide the notice.

This proposed provision would implement CFPA section 1033(a) by clarifying that a data provider does not violate its general obligations to make data available if it provides to consumers a reasonable revocation request. Materially interfering with a consumer's, and therefore an authorized third party's, ability to access the consumer's data would not carry out the objectives of CFPA section 1033(a)'s requirement that data providers make covered data available to a consumer upon request.

6. Public Disclosure Requirements (§ 1033.341)

To facilitate the ability of third parties to request covered data through a developer interface, the CFPB is proposing procedures under CFPA section 1033(a) and, for certain provisions discussed below, CFPA section 1032, to require data providers to publish in a readily identifiable manner certain information about themselves, including identifying information, contact information, and information about their developer interfaces. These provisions would carry out the objectives of CFPA section 1033 by ensuring that consumers and authorized third parties have information necessary to make requests and use a developer interface, which would also promote the use and development of standardized formats available through the developer interface.

Public disclosure of this information would reduce search costs for third parties by giving third parties a low-cost way of identifying how to access a data provider's interface and would facilitate market monitoring by the CFPB and members of the public. The public disclosure of this information would also enable standard-setting bodies to identify the data providers and third parties that are participating in the open banking system, which could aid efforts by standard-setting bodies to develop qualified industry standards related to consumer-authorized access. The CFPB seeks comment on whether data providers should have to disclose additional information beyond the information outlined in proposed § 1033.341. The CFPB also seeks comment on whether data providers should have to periodically provide information exclusively to the CFPB beyond the information it must make public, to support the CFPB's mandate to monitor consumer financial markets for risks to consumers; for example, the CFPB seeks comment on whether data providers should be required to provide the CFPB with annual reports listing the third parties that accessed their systems, the volume of requests they received from such third parties, and copies of certain records retained pursuant to proposed § 1033.351(d), which contains record retention obligations for data providers.

Public Disclosure and Human- and Machine-Readability Requirements (§ 1033.341(a))

Proposed § 1033.341(a) would require data providers to make the information described in proposed § 1033.341(b) through (d) readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website. A data provider would comply with proposed § 1033.341(a)(1) by making the information available on a public website. A data provider would also be permitted to make the information readily identifiable through some other means, as long as the information is no less available than it would be on a public website. Under proposed § 1033.341(a)(2), this information must be available in both human- and machine-readable formats.

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 would make the process of obtaining this information more efficient. The CFPB seeks 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,

[107] *See* 42 U.S.C. 300jj–52(a).

the CFPB seeks 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. For example, the CFPB could require that the information set forth in proposed § 1033.341(b) through (d) be made available on a public website and could require the URL to contain specified text in accordance with the ''well-known Uniform Resource Identifier'' protocol.

Disclosure of Identity Information and Contact Information (§ 1033.341(b))

Proposed § 1033.341(b) would 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; the State in which they are incorporated; and their LEI. This information would help third parties confirm the identity of a particular data provider whose interface it seeks to access. It would also help third parties link the information disclosed by data providers pursuant to proposed § 1033.341 to a particular data provider, particularly where data providers have similar names.

Proposed § 1033.341(b)(4) would require data providers to disclose contact information that enables a consumer or third party to receive answers to questions about accessing covered data under this proposed rule. The CFPB understands that, in the market today, third parties sometimes encounter challenges with accessing data providers' interfaces for consumer-authorized data access. Requiring data providers to disclose this kind of contact information would make it easier for third parties and data providers to resolve such challenges.

Disclosure of Developer Interface Documentation and Access Location (§ 1033.341(c))

The CFPB proposes to require in § 1033.341(c) that a data provider disclose for its developer interface, in the public and readily identifiable 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. It is common practice today for data providers that have built developer interfaces to disclose such metadata and documentation for the interfaces. Where a data provider would need to build (or enhance) its developer interface to comply with the CFPB's proposed rule, a requirement to publicly disclose the associated documentation and metadata would not materially increase the data provider's cost. At the same time, public disclosure of the information would substantially enhance the usability of the interface.

The CFPB proposes to keep simple and high-level the proposed requirement that data providers disclose their interfaces' metadata and documentation, because, as noted, the industry practice of publishing metadata and documentation for data providers' interfaces for third parties is already common. Moreover, the specific formats of the data fields that data providers make available through their interfaces for third parties may continue to evolve, including through qualified industry standards, such that a more detailed requirement could become outdated.

Disclosure of Developer Interface Performance Metrics (§ 1033.341(d))

The CFPB proposes to require in § 1033.341(d) that a data provider disclose, in the public and readily identifiable manner described in proposed § 1033.341(a), the performance of its developer interface for each month. Specifically, the CFPB proposes that on or before the tenth calendar day of each month, the data provider would disclose the percent of requests for covered data received by its developer interface in the preceding calendar month for which the interface provided a proper response, as defined in proposed § 1033.311(c)(1)(i). For example, the data provider would disclose by September 10, 2025, the percent of requests for covered data received by its developer interface in August 2025 for which the interface provided a proper response.

Proposed § 1033.311(c)(1)(i) would set forth the method for calculating the response rate, which would be used for both the substantive requirement and the disclosure requirement.

The CFPB proposes this requirement that a data provider publicly disclose the monthly performance of its developer interface pursuant to section 1032 of the CFPA, which authorizes the CFPB to prescribe disclosures regarding the features of any consumer financial product or service. Because CFPA section 1033(a) requires a data provider to make data available to a consumer when the data ''concern[s] the consumer financial product or service that the consumer obtained from [the data provider],'' the CFPA section 1033(a) requirement that a data provider make the data available to the consumer is itself a feature of the consumer financial product or service that the data provider provided to the consumer. Moreover, the CFPB's section 1032 authority under the CFPA is not limited to disclosures to consumers individually; instead, the section authorizes the CFPB to require disclosures to consumers generally, as well as to potential consumers. Thus, pursuant to its authority provided by CFPA section 1032, the CFPB is proposing in § 1033.341(d) to require a data provider to disclose, in a public and readily identifiable manner, the performance of its interface. The CFPB seeks comment on whether it 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.[108]

7. Policies and Procedures (§ 1033.351)

Reasonable Written Policies and Procedures (§ 1033.351(a))

Proposed § 1033.351(a) would set forth the 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, including proposed § 1033.351(b) through (d). The CFPB proposes § 1033.351(a) pursuant to its authority provided by CFPA sections 1033(a) and 1022(b)(1). The proposed policies and procedures in § 1033.351(b) would 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. The proposed policies and procedures in § 1033.351(c) would carry out the objectives of CFPA section 1033(a) that data be made available in a usable electronic form by ensuring developer interfaces accurately

[108] *See, e.g.,* Australia Consumer Data Standards, *Reporting Requirements, https://consumerdatastandardsaustralia.github.io/standards/#reporting-requirements* (last visited Oct. 11, 2023); Open Fin. Brazil, *Dashboards—Registration and transactional data, https://dashboard.openfinancebrasil.org.br/transactional-data/api-requests/evolution* (last updated Sept. 15, 2023); Open Banking Ltd., *MI Reporting Data API Specification, https://openbankinguk.github.io/mi-docs-pub/v3.1.10-aspsp/specification/mi-data-reporting-api-specification.html#_3-7-daily-volumes-obie* (last visited Oct. 11, 2023).

transmit covered data. In addition, the CFPB is proposing recordkeeping requirements under CFPA section 1022(b)(1) to facilitate supervision and enforcement of the rule and to prevent evasion.

Proposed § 1033.351(a) would further carry out these purposes by requiring that data providers periodically review these policies and procedures and update them as appropriate to ensure their continued effectiveness. To minimize impacts on data providers, including avoiding conflicts with any overlapping compliance obligations, proposed § 1033.351(a) would allow data providers to tailor these policies and procedures to the size, nature, and complexity of their activities.

Policies and Procedures for Making Covered Data Available and Responding to Requests (§ 1033.351(b))

Proposed § 1033.351(b) would require that the policies and procedures required by proposed § 1033.351(a) be reasonably designed to create a record of the data fields made available according to the covered data definition, ensure certain standards are met when not making covered data available, ensure that the data provider communicates certain information to the consumer or third party when declining to provide certain covered data and to ensure reasonably timely communication by the data provider to the consumer when declining to provide certain information.

Making Covered Data Available (§ 1033.351(b)(1))

Proposed § 1033.351(b)(1) would require a data provider to create a record of the data fields that are covered data in the data provider's control or possession. It would also require 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. A data provider is permitted to comply with this requirement by incorporating the data fields defined by a qualified industry standard, but 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 is proposing these requirements to facilitate compliance with and enforcement of the general obligation in proposed § 1033.201. 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. Documentation of use of the exceptions can help identify noncompliant use of the statutory exceptions, while ensuring that data providers can continue to comply with their risk management obligations by giving data providers flexibility to design their own reasonable policies and procedures that comply with the general framework outlined in the proposed rule. The CFPB preliminarily concludes 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).

Denials of Requests for Developer Interface Access and Requests for Information (§ 1033.351(b)(2) and (3))

Proposed § 1033.351(b)(2) would require a data provider to design its policies and procedures reasonably to ensure that any decision to deny a third party's request for access to a developer interface pursuant to proposed § 1033.321 is substantiated in a record and communicated to the third party, as quickly as practicable, in an electronic or written form with the basis for denial. Proposed § 1033.351(b)(3) would require a data provider to design its policies and procedures reasonably to ensure that any decision to deny a consumer or third party's request for information is substantiated in a record and communicated to the consumer or authorized third party in a written or electronic form with the type(s) of information denied and the basis for the denial, and communicated as quickly as practicable. These provisions generally would enable consumers and third parties to understand reasons for denials in a timely manner, and reduce the potential for pretextual denials. These provisions would 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. And, as authorized under section 1022(b)(1) of the CFPA, these provisions also would 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 the proposed rule, permissible bases for a decision to deny access to an interface would include the following: the information requested is not covered data, the information requested is not in the data provider's control or possession, the information requested falls into one of the exceptions outlined in proposed § 1033.221, the request does not satisfy the conditions for access under proposed § 1033.331, the data provider is reasonably denying access based on risk management concerns for reasons described in proposed § 1033.321, or the data provider's interface is not available when received a request, as described in proposed § 1033.331(c)(3).

The provisions would give data providers flexibility to comply with their data security or risk management obligations—a concern identified by small entity representatives during the SBREFA process. For example, in some cases a data provider might deny a third party's request for interface access because of a specific risk management issue under § 1033.321. The CFPB understands that in limited cases, the disclosure of the specific reason for a denial might present additional risk management concerns. The proposed rule would give data providers flexibility to design policies and procedures to reasonably account for such issues. The CFPB requests 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.

Policies and Procedures for Ensuring Accuracy (§ 1033.351(c))

Proposed § 1033.351(c) would require data providers to establish and maintain policies and procedures reasonably designed to ensure the accuracy of covered data made available through the data provider's developer interface. The proposed rule also lists elements that data providers would need to consider when designing their policies and procedures. Proposed § 1033.351(c) would be authorized under CFPA section 1033(a) for the reasons stated above in the discussion of proposed § 1033.351(a) as well as under CFPA section 1033(d). Policies and procedures for accuracy would promote the use and development of standardized formats by ensuring data providers are taking reasonable measures to share covered data in standardized formats.

As discussed in part I.D, one of the goals of the proposed rule is to foster a data access framework that operates reliably. The accurate transfer of

consumer financial data is important to the operation of an open banking system and to consumers' ability to benefit from the data access right in CFPA section 1033. If data providers fail to reliably transfer data that accurately reflects the information they possess in their systems, then third parties will struggle to develop innovative, or even functional, financial products and services. And consumers will face difficulty finding any benefit from sharing their data with competing financial service providers. For these reasons, proposed § 1033.351(c)(1) would require data providers to establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface.

The CFPB has 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. That is, 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 information stored in data providers' existing systems is likely subject to several legal requirements regarding accuracy. For example, Regulation E protects consumers against errors, and Regulation Z protects consumers against billing errors.[109] In addition, the Interagency Guidelines Establishing Standards for Safety and Soundness require operational and managerial standards for information systems.[110] Additionally, many small entity representatives and other stakeholders commenting on the SBREFA Outline cited the transfer of data from data providers to third parties as a source of inaccuracies. Many transfer issues will be addressed by the performance specifications for a data provider's developer interface in proposed § 1033.311(c), but policies and procedures specifically concerning accuracy would help prevent errors not addressed by the other proposed performance standards, as discussed below.

The flexible standard proposed would allow data providers to design systems that are better adapted to the context of their developer interface, including changes in technology and the size, nature, and complexity of the data provider's activities. It would also allow data providers to leverage any knowledge developed through designing or administering systems for ensuring the accuracy of financial information under existing accuracy standards. Many of the other regulations governing the accuracy of similar financial information on data providers' systems incorporate flexible standards.

Proposed § 1033.351(c)(2) provides two elements for data providers to consider when developing their policies and procedures regarding accuracy: (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. Although reasonable policies and procedures would address many elements, the two identified in the proposed rule seem especially relevant to an assessment of whether a data provider's policies and procedures are reasonable. Implementing the proposed formatting requirements would help prevent inaccuracies that might be introduced by translating covered data between various unstandardized formats. And addressing information from a consumer or third party is relevant to the reasonableness of a data provider's policies and procedures because these parties are likely to know whether information has been accurately transferred to the products or services they are using or providing. These elements should help data providers design their policies and procedures without negating the flexibility described above, because the implementation of each element will depend on context. For example, in considering information submitted by a consumer or third party, a data provider might create certain policies regarding irrelevant or duplicative requests, or certain policies regarding which requests require further communication with the consumer or third party.

Proposed § 1033.351(c)(3) states that indicia that a data provider's policies and procedures regarding accuracy are reasonable include whether they conform to a qualified industry standard regarding accuracy. 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 seeks comment on whether the final rule should include additional elements bearing on the reasonableness of a third party's policies and procedures regarding accuracy.

Policies and Procedures for Record Retention (§ 1033.351(d))

Proposed § 1033.351(d) would require that data providers establish and maintain policies and procedures reasonably designed to ensure retention of records that evidence compliance with their obligations under proposed subparts B and C. This provision would clarify the policies and procedures data providers must maintain to ensure the CFPB and other enforcers can verify compliance with the proposed rule. The specific requirements proposed in § 1033.351(d) would facilitate supervision and enforcement of the proposed rule by the CFPB, Federal and State banking regulators, State attorneys general, and other government agencies that supervise data providers.

The CFPB has preliminarily determined the proposed retention periods in § 1033.351(d)(1), beginning once the data provider makes the data available to the consumer or third party under CFPA section 1033(a), will provide a sufficient amount of time to supervise whether the data was made available while not unduly burdening data providers. Additionally, the proposed requirement to retain records for a minimum of three years after a data provider has responded to a consumer's or third party's request for information or a third party's request to access a developer interface would provide sufficient time to administer enforcement of proposed subparts B and C. All other records that are evidence of compliance with the proposed rule would need to be retained for a reasonable period of time. The CFPB requests comment on proposed § 1033.351(d) regarding the length of the retention period and the date from which the retention obligation should be measured.

Proposed § 1033.351(d) would provide flexibility to data providers by establishing a minimum retention period and by not exhaustively specifying categories of records. The proposed requirements are unique to CFPA section 1033 and provide data providers with 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), rather than the policies and procedures that are appropriate to the industry at large. Further, this flexibility would help data providers avoid conflicts with other legal obligations (including record retention and data security obligations), manage data security risks, and minimize unnecessary impacts. To

[109] *See* 12 CFR part 1005; 12 CFR 1026.13.

[110] *See, e.g.,* 12 CFR part 208, app. D–1.

mitigate the risk that this flexibility might result in the absence of critical evidence of compliance, proposed § 1033.351(d)(2) would identify particular examples records that would need to be retained. The CFPB requests comment as to the types of records that should be retained to evidence compliance. This approach 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.[111]

CFPA section 1022(b)(1) 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. Proposed § 1033.351(d) would assist the CFPB with administering CFPA section 1033 by ensuring records are available to evaluate compliance with data providers' obligations under the proposed rule. Additionally, such requirements will also help data providers in assessing their own compliance with the requirements of CFPA section 1033. Further, the requirement proposed in § 1033.351(d) for data providers to establish and maintain policies and procedures to retain records of all evidence of compliance with the applicable requirements in the proposed rule would make it more difficult for data providers to evade the requirements of CFPA section 1033. Consequently, proposed § 1033.351(d) would both allow the CFPB and other entities with CFPA enforcement authority to enforce CFPA section 1033, and discourage evasion by data providers, thus meeting both requirements for CFPA section 1022(b)(1) authorization.

CFPA section 1033(c) 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.'' The CFPB has preliminarily determined that proposed § 1033.351(d) is consistent with CFPA section 1033(c) because CFPA section 1033(c) merely provides that a covered person is not required to maintain or keep additional information on a consumer and is silent as to record retention relating to compliance with CFPA section 1033 itself. Thus, the statute neither precludes the CFPB from adopting retention requirements nor overrides other authorities at the CFPB's disposal to impose reasonable record retention obligations. Accordingly, because the authority for proposed § 1033.351(d) arises from CFPA section 1022(b)(1) and is necessary for the CFPB and others with enforcement authority to verify data provider's compliance with CFPA section 1033, the CFPB is authorized to require data providers to establish and maintain policies and procedures to ensure the retention of records that evidence compliance with their obligations under proposed subparts B and C.

D. Subpart D—Authorized Third Parties

1. Overview

The CFPB is proposing authorization procedures for third parties seeking to access covered data on consumers' behalf. Section 1033(a) of the CFPA generally requires data providers to make information available to a consumer and agents, trustees, or representatives acting on their behalf. The proposed authorization procedures are designed to ensure that third parties accessing covered data are acting on behalf of the consumer. Specifically, the proposed authorization procedures would include requirements to provide an authorization disclosure to inform the consumer of key terms of access, certify to the consumer that the third party will abide by certain obligations regarding the consumer's data, and obtain the consumer's express informed consent to the key terms of access contained in the authorization disclosure. The CFPB is proposing specific requirements that would apply when the third party is using a data aggregator. Proposed subpart D would also contain requirements relating to retention of evidence of compliance with proposed subpart D.

2. Third Party Authorization Procedures (§ 1033.401)

The CFPB is proposing that a third party acting on behalf of a consumer would be able to access covered data. Proposed § 1033.201(a) provides that a data provider must make covered data available to a consumer and an authorized third party, and proposed § 1033.401 specifies what requirements a third party must satisfy to become an authorized third party that is entitled to access covered data on behalf of a consumer. These 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. They would also help ensure that the third party will take appropriate steps to protect the consumer's data and that the consumer will provide express informed consent for the third party to collect, use, and retain the covered data. 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 used in section 1033.

The CFPB is proposing in § 1033.401 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 requirement is 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.

The CFPB is also proposing in § 1033.401 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: (1) provide the consumer with an authorization disclosure as described in proposed § 1033.411; (2) provide a statement to the consumer in the authorization disclosure certifying that the third party agrees to certain obligations described in proposed § 1033.421; 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.

The proposed requirement in § 1033.401(a) that a third party provide an authorization disclosure to the consumer would 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 authorization disclosure is discussed in more detail below.

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. As noted below, proposed § 1033.411(b)(5) would require the third party to include the certification statement in the authorization disclosure. Among other things, the third party would agree that it will comply with limitations on collection, use, and retention of the consumer's

[111] SBREFA Panel Report at 45.

data; comply with certain data privacy restrictions; take certain steps to ensure data accuracy and security; and take certain steps to ensure consumers are informed about the third party's access to covered data and the consumer's ability to revoke that access. These proposed third party obligations are set forth in proposed § 1033.421 and are discussed in more detail below.

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. Proposed § 1033.401(c) specifies that, to obtain express informed consent, the third party must obtain an authorization disclosure that is signed by the consumer electronically or in writing. Proposed § 1033.421(g)(1) would require the third party to provide the consumer with a copy of the signed authorization disclosure.

The SBREFA Panel recommended that the CFPB consider how to design authorization procedures that minimize costs on third parties while still achieving the CFPB's objective of helping to ensure that consumers provide express informed consent when authorizing third parties to access their information.[112] In the proposed rule, the CFPB has attempted to balance these considerations in developing the proposed authorization procedures. The SBREFA Panel also recommended that the CFPB consider how the third party authorization procedures interact with data providers' obligations to make information available.[113] As explained above, proposed § 1033.331(b) provides the circumstances in which a data provider would be required to make available covered data to a third party, including when it has received information sufficient to, among other things, confirm that the third party has followed the authorization procedures in proposed § 1033.401.

In addition, the SBREFA Panel recommended that the CFPB consider how the third party authorization procedures would work in the context of accounts with multiple owners. As discussed above in connection with proposed § 1033.331(d), the CFPB is proposing 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 requests 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 requests 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 also requests comment on whether the authorization disclosure, including the statement that the third party will comply with certain third party obligations, is 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 requests 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, proposed § 1033.401 would apply a consistent set of procedures to all third parties attempting to access covered data. The CFPB understands, however, that the proposed authorization procedures might not be appropriate for some third parties, particularly smaller or non-commercial parties, that might need access to a consumer's covered data. The CFPB requests comment about whether there are certain third parties for whom proposed § 1033.401 would not be appropriate. Additionally, the CFPB requests comment about whether the proposed authorization procedures described in proposed § 1033.401 should be streamlined for certain third parties. The CFPB also requests 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 requests comment on how individuals who are not account owners currently use existing legal mechanisms to directly access covered data.

3. Authorization Disclosure (§ 1033.411)

The CFPB is proposing that third parties would be required to provide consumers with authorization disclosures, as described in proposed § 1033.401, to be authorized to access covered data on behalf of consumers. The purpose of the authorization disclosure is to provide consumers with key terms of access so they can make informed decisions about granting third party access to covered data and to therefore ensure that third parties are acting on behalf of consumers. Consistent with the SBREFA Panel recommendation that the CFPB consider how it can reduce compliance costs for third parties in providing the authorization disclosure by further specifying the content and formatting principles of the disclosure, proposed § 1033.411 specifies format and content requirements for the authorization disclosure.[114]

General Requirements (§ 1033.411(a))

Proposed § 1033.411(a) would require the third party to provide the consumer with an authorization disclosure electronically or in writing. Proposed § 1033.411(a) also sets forth the general format requirements for the authorization disclosure. Specifically, the CFPB is proposing that the authorization disclosure must be clear, conspicuous, and segregated from other material. The proposed provisions would help ensure the authorization disclosure is provided in a format that facilitates consumer understanding of the key terms of access. The CFPB has preliminarily determined that these requirements, which are consistent with standards used in other consumer financial services laws and their implementing regulations,[115] would facilitate consumer understanding of the authorization disclosure. The CFPB considered how to facilitate compliance with existing disclosure requirements, such as disclosures required by Regulation P of the GLBA, as recommended by the SBREFA Panel.[116] The CFPB has preliminarily determined that requiring the authorization

[112] *Id.* at 44.

[113] *Id.* at 43.

[114] *Id.*

[115] For example, Regulation F requires notices for validation of debts to be clear and conspicuous, which it defines as ''readily understandable'' and ''[i]n the case of written and electronic disclosures, the location and type size also must be readily noticeable and legible to consumers, although no minimum type size is mandated.'' 12 CFR 1006.34(b)(1); Regulation Z requires both open-end credit and closed-end credit disclosures to be clear and conspicuous, and it requires closed-end credit disclosures to grouped together and segregated from everything else. 12 CFR 1026.5(a)(1)(i), 1026.17(a)(1).

[116] SBREFA Panel Report at 43.

disclosure to appear segregated from other required disclosures 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 seeks comment on whether these formatting requirements would aid consumer understanding and whether additional requirements should be included in the rule. Specifically, the CFPB seeks comment on whether the rule should contain more prescriptive requirements, such as a word count or reading level, and whether additional requirements are needed to ensure that the authorization disclosure content is provided in a standalone format. The CFPB also seeks 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 seeks 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.

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 would already require that the authorization disclosure be provided in an accessible format.[117] The CFPB seeks comment on whether the rule should contain requirements relating to the accessibility of the authorization disclosure.

Authorization Disclosure Content (§ 1033.411(b))

Proposed § 1033.411(b) would require 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). In addition to the authorization disclosure content requirements in proposed § 1033.411(b), proposed § 1033.431(b) would require the authorization disclosure to include the name of any data aggregator that will assist the third party with accessing covered data and a brief description of the services the data aggregator will provide.

In proposing content requirements for the authorization disclosure, the CFPB aims to strike a balance between providing consumers with sufficient information to enable informed consent to data access and keeping the disclosure short to increase the likelihood that consumers will read and understand it. The CFPB preliminarily concludes 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 seeks comment on any obstacles to including the proposed authorization disclosure content and on whether additional content is needed to ensure consumers have enough information to provide informed consent. Specifically, the CFPB seeks 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 seeks comment on alternative disclosures that would achieve the CFPB's objective, and 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).

Language Access (§ 1033.411(c))

Proposed § 1033.411(c)(1) would require the authorization disclosure to be in the same language as the communication in which the third party conveys the authorization disclosure to the consumer and would require any translation of the authorization disclosure to be complete and accurate. Under proposed § 1033.411(c)(2), if the authorization disclosure is in a language other than English, it would be required to include a link to an English-language translation and would be permitted to include links to translations in other languages. Additionally, if the authorization disclosure is in English, it would be permitted to include links to translations in other languages.

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 has 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. Accordingly, proposed § 1033.411(c)(1) would require the authorization disclosure to be in the same language as the communication in which the third party conveys the authorization disclosure to the consumer, and proposed § 1033.411(c)(2) would permit, but not require, the authorization disclosure to include links to translations of the authorization disclosure in languages other than English.

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. English-language disclosures may also allow consumers to confirm the accuracy of the translation. For these reasons, proposed § 1033.411(c)(2) would require that an authorization disclosure in a language other than English include a link to an English-language translation.

The CFPB seeks comment on whether the proposed language access provisions would adequately decrease the risk that consumers with limited English proficiency may be given information in a manner that impedes informed consent while not imposing unduly burdensome requirements on third

[117] *See* 42 U.S.C. 12132, 12182(a); 28 CFR 35.130, 35.160(a), 36.201, 36.303(c).

parties. The CFPB also seeks comment on whether the rule should include any requirements regarding consistency of the language of the authorization disclosure and other communications related to the product or service provided by the third party, and whether the rule should clarify how language access requirements apply if the consumer has not engaged with the third party electronically.

4. Third Party Obligations (§ 1033.421)

Proposed § 1033.421 would describe the obligations to which third parties must certify to be authorized to access covered data. The CFPB is proposing these certification requirements to ensure that third parties accessing covered data are acting on behalf of the consumer. The proposal would require third parties to certify to limit their collection, use, and retention of covered data, including limiting the duration and frequency of collection and the provision of data to other third parties, to what is reasonably necessary to provide the consumer's requested product or service. Under proposed § 1033.421, third parties would certify to a maximum duration of collection of one year after the consumer's authorization unless the consumer reauthorizes the third party's access. Third parties would also be required to certify to provide consumers a simple way to revoke access, to maintain certain accuracy and data security obligations, and to ensure consumers have access to information about the third party's authorization to access data. Proposed § 1033.421 would also require a certification related to providing covered data to another third party and would provide requirements that apply when the third party is using a data aggregator.

General Standard To Limit Collection, Use, and Retention (§ 1033.421(a))

Under proposed § 1033.421(a)(1), third parties would be 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 provide that, for purposes of the limitation in § 1033.421(a)(1), certain activities are not part of, or reasonably necessary to provide, any other product or service. Under the proposal, 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.

In the SBREFA Outline, the CFPB stated that it was considering proposing that third parties limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service.[118] The SBREFA Panel recommended the CFPB consider options for collection, use, and retention that do not unnecessarily restrict third parties' ability to provide consumers with requested products or services.[119] The SBREFA Outline also requested feedback on potential approaches to specifically limit third parties' use of covered data.[120] One option would not have permitted third parties to use covered data for purposes not reasonably necessary to provide the consumer's requested product or service (secondary use).[121] Other options would have allowed third parties to ask consumers to opt in to or opt out of secondary uses, including an approach that would not have permitted third parties to ask consumers to opt in to certain ''high-risk'' secondary uses.[122] The SBREFA Panel recommended that the CFPB consider where it can give flexibility to third parties while still achieving its consumer protection objectives.[123]

The proposed limit on collection, use, and retention in § 1033.421(a) is designed to ensure that, consistent with carrying out the objectives of CFPA section 1033, third parties accessing covered data are acting on behalf of consumers, thereby ensuring that their collection, use, and retention of covered data proceeds in alignment with consumer control and truly informed consent. Specifically, the proposal is 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 and not reluctantly acquiescing to data collection, use, and retention that they do not want. Further, the CFPB notes that covered data that third parties would collect, use, and retain pursuant to consumer authorization includes sensitive financial data that might expose consumers to fraud or identity theft if it were exposed.[124] The proposed limitation in § 1033.421(a) is designed to ensure that third parties act on behalf of consumers when accessing that sensitive data. For the reasons described below, the CFPB preliminarily concludes that proposed § 1033.421(a), including the proposal to prohibit secondary uses of covered data, would appropriately ensure that third parties accessing covered data are acting on behalf of consumers, while providing sufficient flexibility to third parties to provide consumers with their requested products or services.

The CFPB seeks comment on whether there are technology-based solutions that could apply the appropriate proposed third party requirements automatically. For example, the CFPB seeks comment on whether such solutions are available that could assist third parties with automatically terminating access after the third party's authorization has ended or with limiting the use of covered data consistent with the limitation described in proposed § 1033.421(a). If such solutions are available, the CFPB requests comment on whether to require third parties to integrate these capabilities.

Reasonably Necessary

Proposed § 1033.421(a)(1) would provide that third parties must limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. The ''reasonably necessary'' standard in proposed § 1033.421(a)(1) is similar to standards in several data privacy frameworks that minimize third parties' collection, use, and retention of data.[125] The proposed ''reasonably necessary'' standard is designed to ensure that the consumer is the primary beneficiary of any authorized data access, and that accordingly the resulting collection, use and retention of data proceeds in alignment with true consumer control and informed consent.

Congress intended that, through CFPA section 1033, the consumer would have the right to access their covered data for their own benefit. As a representative acting on behalf of the consumer, a third

[118] SBREFA Outline at 41.

[119] SBREFA Panel Report at 44.

[120] SBREFA Outline at 43.

[121] *Id.*

[122] *Id.*

[123] SBREFA Panel Report at 45.

[124] 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.

[125] *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.''); Colo. Rev. Stat. section 6–1–1308(4) (2021) (''A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.'')

party authorized to access the consumer's covered data must ensure that the consumer is the primary beneficiary of such access. Third parties can benefit from access as well, but only by collecting, using and retaining data as reasonably necessary for the primary purpose for which the consumer entered the market. The CFPB preliminarily concludes that collection, use, or retention of covered data beyond what is reasonably necessary to provide the consumer's requested product or service risks positioning the third party as the primary beneficiary of data access and, generally, will not be consistent with meaningful consumer control over data collection, use and retention.

Further, as a representative acting on behalf of the consumer, third parties accessing covered data should ensure consumers are best positioned to understand the scope of their authorizations and their effect on third party collection, use, and retention. The CFPB preliminarily concludes 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. The CFPB also preliminarily concludes that collection, use, and retention of covered data under these circumstances would undermine a consumer's ability to control their data.

The CFPB considered a number of alternatives to the ''reasonably necessary'' standard, including by evaluating data collection, use, and retention limitations in other data privacy regimes. 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 has preliminarily determined that, among other standards the CFPB considered, a ''reasonable necessity'' 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.

Consumer's Requested Product or Service

Proposed § 1033.421(a)(1) is also designed to carry out the objectives of CFPA section 1033 by limiting collection, use, and retention of covered data to the product or service the consumer requested.

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. However, third parties can significantly benefit from accessing consumers' covered data, and consumers often do not know about various data uses,[126] do not want companies to use their data broadly,[127] and also generally lack bargaining power to engage in the market while protecting their data privacy.[128] As a result, third parties often broadly collect, use, and retain covered data in ways that are for their own benefit. To ensure that entities only collect, use, and retain data on consumers' behalf, pursuant to informed consent, the CFPB is limiting data collection, use, and retention to what is reasonably necessary to provide a requested product or service. To avoid circumvention of that standard, the CFPB will treat the product or service as the core function that the consumer sought in the market and that accrues to the consumer's benefit. For example, the scope of the product or service is not defined by disclosures, which 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 chooses that would often benefit the third party and not the consumer. The CFPB preliminarily determines that the proposed approach would 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.[129]

Targeted Advertising, Cross-Selling, and Data Sales

To further ensure that third parties accessing covered data are collecting, using, and retaining that data only to provide the product or service the consumer requested, proposed § 1033.421(a)(2) provides that, for purposes of proposed § 1033.421(a)(1), certain activities—targeted advertising, cross-selling of other products or services, or the sale of covered data—are not part of, or reasonably necessary to provide, any other product or service. The CFPB has preliminarily determined that when the consumer goes into the market seeking such other products or services—such as a loan, a checking account, or a personal financial management tool—the use of data for the purposes identified in proposed § 1033.421(a)(2) is, as a general matter, not for the primary benefit of the consumer.[130] Therefore, the CFPB

[126] *See* April Falcon Doss, *Cyber Privacy,* at 61 (BenBella Books, Inc. 2020) (explaining that it is difficult for consumers to understand what they are consenting to, how their data might be collected and used, how it might be sold to others, what the impacts of aggregation are, etc.); Ramy El-Dardiry *et al., Brave New Data: Policy Pathways for the Data Economy in an Imperfect World,* CPB Netherlands Bureau for Econ. Policy Analysis at 10 (2021), *https://www.cpb.nl/sites/default/files/omnidownload/CPB-uk-Policy-Brief-Brave-new-data.pdf* (''Consumers cannot see what companies are doing with their data, nor can they read all of the data terms of use or oversee the consequences. Companies are able to exploit their strong informational position by manipulating the preferences of consumers and enticing them to . . . sell more data.'')

[127] *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/* (stating that 81 percent of consumers feel the risks outweigh the benefits of companies collecting data about them and that 79 percent of consumers are very or somewhat concerned about how companies use data).

[128] *See* Yosuke Uno *et al., The Economics of Privacy: A Primer Especially for Policymakers,* at 16, Bank of Japan Working Paper No. 21–E–11 (Aug. 2021), *https://www.boj.or.jp/en/research/wps_rev/wps_2021/data/wp21e11.pdf* (stating that consumers cannot ''truthfully express the degree of privacy protection they desire,'' because companies put consumers ''in a situation where it becomes optimal for them not to choose stronger privacy protection, even though they prefer it''); Ramy El-Dardiry *et al., Brave New Data: Policy Pathways for the Data Economy in an Imperfect World,* at 10, CPB Netherlands Bureau for Econ. Policy Analysis (2021), *https://www.cpb.nl/sites/default/files/omnidownload/CPB-uk-Policy-Brief-Brave-new-data.pdf* (''People are consciously, and unconsciously, providing data, *e.g.,* when they consume a digital service . . . but often have limited control over or insight into how their data are used by data processors. This unequal balance of power has several causes: market power, information asymmetry and behavioural biases. As a result, mainly the data processors determine, within the legal framework, which personal data are collected and how they are used, rather than the party supplying the data.'')

[129] *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%) or often (13%) 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 consumer 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.'')

[130] Accordingly, the proposed rule would not prevent third parties from engaging in an activity

Continued

preliminarily determines 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).

Specifically, the CFPB understands from stakeholder feedback and research that targeted advertising, cross-selling, and data sales do not primarily benefit consumers in most cases for various reasons.[131] The CFPB understands that these activities are pervasive in the market,[132] and that consumers often lack choices about whether their data will be used for these purposes.[133] Stakeholder feedback suggests that consumers often do not expect targeted advertising, cross-selling, and data sales to be part of the product or service they receive or understand these activities' potential for harm. In contrast, third parties can greatly benefit from these activities. Therefore, the CFPB has 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. Combining these activities with other features of a product or service may also interfere with consumers' ability to sufficiently control their data and understand the scope of their authorizations.

Proposed § 1033.421(a)(2) is designed to impose a bright-line rule with respect to targeted advertising, cross-selling of other products or services, and the sale of covered data. However, proposed § 1033.421(a)(2) is not meant to be an exhaustive list of activities that should not be considered part of any other requested product or service, such as data activities described in terms and conditions that are neither the core function that the consumer went into the market to obtain or reasonably necessary to achieve that function. The CFPB also seeks comment on whether activities other than those identified in proposed § 1033.421(a)(2) should be included in the activities listed in proposed § 1033.421(a)(2).

Limitations on Collection of Covered Data (§ 1033.421(b))

Proposed § 1033.421(b) contains third party obligations related to collection of covered data. As described below, 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; (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.

Specifically, proposed § 1033.421(b)(1) would provide that, consistent with proposed § 1033.421(a)(1), third parties must limit their collection—including the scope of covered data collected and the duration and frequency of collection of covered data—to what is reasonably necessary to provide the consumer's requested product or service. The SBREFA Panel recommended that the CFPB consider options to limit duration and frequency of third party collection of consumer data that do not unnecessarily restrict third parties' ability to provide products or services requested by consumers. The Panel also recommended that the CFPB consider the option of limiting third party collection to the duration and frequency necessary based on the product or service requested by consumers. Third parties often obtain significantly more consumer data, for longer periods, than is necessary to provide requested products and services to consumers.[134] The CFPB understands that ongoing data collection can undermine consumer expectations or understanding, and in some cases, can go beyond the consumer's informed consent.[135] The CFPB has preliminarily determined that limiting the scope of data collected, and duration and frequency of data collection, to what is reasonably necessary to provide the consumer's requested product or service would reduce the potential for harm associated with ongoing data collection.

Proposed § 1033.421(b)(1) is responsive to the SBREFA Panel recommendations that the CFPB consider options to limit duration and frequency of third party collection of consumer data that do not unnecessarily restrict third parties' ability to provide products or services requested by consumers, and consider the option of

described in proposed § 1033.421(a)(2) as a stand-alone product. To the extent that 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, of course, would also be subject to all other applicable laws, including the CFPA's prohibition on unfair, deceptive and abusive practices.

[131] *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,* at 1, 5–6, 2 GPH Int'l J. of Bus. Mgmt. (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 risk the data will be breached or that malicious parties will purchase the data on the secondary market).

[132] *See* Rishbah Kirpalani & Thomas Philippon, *Data Sharing and Market Power With Two-Sided Platforms,* at 2, Nat'l Bureau of Econ. Rsch. Working Paper No. 28023 (Dec. 2020), *http://www.nber.org/papers/w28023* (''Large internet platforms have changed the way market participants interact. One reason for this is the extraordinary ability of platforms . . . to gather and analyze large amounts of data. Platforms use this data to enable better matching between participants as well as for commercial purposes, including sale to third parties.''); Daron Acemoglu *et al., Too Much Data: Prices and Inefficiencies in Data Markets,* at 1, Nat'l Bureau of Econ. Rsch. Working Paper No. 26296 (Sept. 2019), *https://www.nber.org/papers/w26296* (''The data of billions of individuals are currently being utilized for personalized advertising or other online services. The use and transaction of individual data are set to grow exponentially in the coming years with more extensive data collection from new online apps and integrated technologies such as Internet of Things and with the more widespread applications of artificial intelligence (AI) and machine learning techniques.'')

[133] *See, e.g.,* Yan Lau, *Economic Issues: A Brief Primer on the Economics of Targeted Advertising,* at 9–10, Bureau of Econ., Fed. Trade Comm'n (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 underestimating the ''degree and consequence of the personal data collection websites carry out in exchange for providing free digital goods and services;'' consumers might feel the benefits of targeted advertising do not outweigh the ''perceived intrusiveness of the advertising''; and consumers might experience harms related to data breaches or misuse of their data).

[134] *See generally* Itay P. Fainmesser *et al., Digital Privacy,* 96 Mgmt. Sci. 3157, 3158 (2022), *https://pubsonline.informs.org/doi/10.1287/mnsc.2022.4513* (describing broad collection and use of consumer data to improve digital businesses and extract increased profits); Daron Acemoglu *et al., Too Much Data: Prices and Inefficiencies in Data Markets,* at 3, Nat'l Bureau of Econ. Rsch. Working Paper No. 26296 (2019), *https://www.nber.org/papers/w26296* (describing a lack of balance in the market between what consumers authorize and what data are collected and how data are used).

[135] *See generally* April Falcon Doss, *Cyber Privacy,* at 50 (BenBella Books, Inc. 2020) (''First, data asymmetry is endemic. Data subjects rarely know as much as data holders do about what's being collected and how it's being used. Second, data subjects seldom have complete visibility into, or a full appreciation of, the complex interactions among the many ways that data can be used. Third, even with that information and appreciation, consumers find their choices are limited.'')

limiting third party collection to the duration and frequency necessary based on the product or service requested by consumers.[136]

Maximum Duration

Proposed § 1033.421(b)(2) would provide that third parties must limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent reauthorization.

In the SBREFA Outline, the CFPB stated that it was considering proposing that third party authorization to access covered data would be limited to a maximum period.[137] The CFPB also asked whether it should consider other provisions related to a maximum durational period, including a proposal that would require all authorized third parties to obtain reauthorization on the same day or during the same month each year, for all consumers.[138] The CFPB received a range of feedback related to limiting third party authorization to a maximum durational period. Many commenters were generally supportive of the approach but suggested variations, such as not allowing third parties to collect consumer data longer than necessary to satisfy a legitimate purpose, or requiring third parties to end their collection of consumer data after a period of consumer inactivity, *i.e.,* ''dormancy.'' Other commenters supported a maximum duration on collection, citing concern that limiting collection of consumer data to what is reasonably necessary for the product or service, on its own, would not go far enough to ensure that third parties adhere to consumer preferences related to privacy, because third parties could wrongfully extend collection without sufficient bases. Other commenters stated that a maximum limitation on duration would result in undesired loss of services for consumers or might otherwise frustrate consumer intent.

The CFPB recognizes that some products or services, like bill pay, overdraft prevention, or personal financial management, require long term access. For products or services that require ongoing data collection, the general limitation standard may not be sufficient to ensure that third parties act on behalf of consumers when collecting data over the longer term. For example, 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. 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, there will be 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, it would frustrate consumer intent and burden third parties to terminate third party access or require frequent reauthorizations.

The CFPB has preliminarily determined that requiring third parties to limit data collection to a maximum durational period would effectively account for the concern that long-term data collection may not align with consumer expectations in some cases. Under proposed § 1033.421(b)(2), even if consumers do not request revocation as described in proposed § 1033.421(h), third party authorization would end after the maximum period ends and the consumer does not reauthorize. The CFPB has also preliminarily determined that one year is an appropriate period for the maximum duration of collection. This approach could provide an effective check against data collection that consumers no longer need or want, while avoiding burdens associated with shorter maximum durational periods, such as frequent requests for reauthorization.

The CFPB considered whether to propose an explicit limit on duration related to dormancy, as suggested by some commenters. The CFPB has preliminarily determined that a dormancy approach could be burdensome for third parties to operationalize as they may not have a clear view into a consumer's activity, and that some of the benefits of a dormancy period could be achieved by a maximum durational period. The CFPB seeks comment on dormancy, including about how a dormancy limitation might work in comparison to a uniform maximum duration, and how dormancy might be operationalized.

Reauthorization

Proposed § 1033.421(b)(3) would require that, to collect covered data beyond the one-year maximum period, the third party will obtain a new authorization from the consumer pursuant to proposed § 1033.401 no later than the anniversary of the most recent authorization from the consumer. Under that proposal, the third party would be permitted to ask the consumer for a new authorization pursuant to proposed § 1033.401 in a reasonable manner. Under the proposal, indicia that the new authorization request is reasonable include its conformance to a qualified industry standard.

In the SBREFA Outline, the CFPB described an approach in which, after the maximum durational period ends, third parties would need to seek reauthorization for continued access, and many commenters supported that approach.[139] The SBREFA Panel recommended the CFPB consider options for reauthorization requirements after the expiration of any durational limitations.[140]

The CFPB has preliminarily determined that consumers would benefit from the ability to provide annual authorizations for third party data access. Annual authorizations would provide a yearly check-in for consumers to take or leave third party data access for products or services they have previously authorized. As such, proposed § 1033.421(b)(3) would allow third parties to seek from consumers new authorizations before the maximum durational period ends to avoid service interruptions or added friction in consumers' user experience with the third party.

Further, the CFPB has preliminarily determined that third parties might need to seek new authorizations multiple times or otherwise explain to consumers why they are seeking new authorizations. The CFPB understands, however, that third parties might unnecessarily burden consumers with many requests for authorization or otherwise attempt to obtain consumer authorizations for third party data access that consumers no longer want. To account for both of these concerns, proposed § 1033.421(b)(3) would allow third parties to seek new authorizations, in a reasonable manner, no later than the anniversary of the consumer's initial authorization. The CFPB has also preliminarily determined that additional guidelines related to reauthorization requests may facilitate compliance for third parties. As such, proposed § 1033.421(b)(3) would provide that indicia that a new authorization request is reasonable include conformance with a qualified industry standard on the subject.

Effects of Maximum Duration (§ 1033.421(b)(4))

Finally, proposed § 1033.421(b)(4) provides that, if the consumer does not provide a new authorization before the maximum durational period ends, third

[136] SBREFA Panel Report at 44.

[137] SBREFA Outline at 41.

[138] *Id.* at 42.

[139] *Id.* at 41.

[140] SBREFA Panel Report at 44.

parties 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. As noted above, proposed § 1033.421(b)(2) would impose a maximum durational period of one year as a check against data collection that consumers no longer need or want. Consistent with proposed § 1033.421(b)(2), proposed § 1033.421(b)(4)(i) specifies that, once the maximum durational period ends and the consumer does not provide a new authorization, the third party may no longer collect covered data pursuant to the consumer's authorization.

Proposed § 1033.421(b)(4)(ii) specifies, 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, 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). 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. 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) would address this concern by making clear that the general limitation on use and retention contained 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.

Proposed § 1033.421(b)(4)(ii) recognizes that, while use and retention of covered data will not be reasonably necessary for most purposes after the maximum durational period ends and the consumer does not provide a new authorization, it may continue in some circumstances. The consumer's failure to reauthorize access beyond the maximum period of one year, all other things being equal, indicates that the existing authorization, without more, no longer supports use or retention of data collected under its terms. In the normal course, therefore, application of the general standard in proposed § 1033.421(a) will call for the third party, after its failure to secure reauthorization, to stop using and retaining data collected pursuant to the earlier authorization. However, specific circumstances may justify continued use and or retention of some or all such data under that standard, even as new collection, use and retention stops. For example, 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. Similarly, 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(b)(4)(ii) even as the consumer no longer makes use of the product in any manner that would require continued data collection.

The CFPB has preliminarily determined that proposed § 1033.421(b)(4)(ii) 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 standard in proposed § 1033.421(a), while ensuring that consumer data are not used and retained, beyond the expiration of the maximum period without reauthorization, in a manner that does not properly reflect the control afforded the consumer under that same general standard. The CFPB seeks comment about these circumstances and whether, following the end of a maximum durational period, additional protections for consumers or flexibilities for third parties are warranted.

Limitations on Use of Covered Data (§ 1033.421(c))

Under proposed § 1033.421(a), use of covered data that is not reasonably necessary to provide the consumer's requested product or service—*i.e.,* secondary uses—would not be permitted as part of the third party's authorization to access the consumer's covered data. Proposed § 1033.421(c) specifies 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 is reasonably necessary to provide the consumer's requested product or service. For clarity, proposed § 1033.421(c) would include the following examples of uses of covered data that would be permitted as reasonably necessary: (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.

As described above, the SBREFA Panel recommended that the CFPB consider how the secondary use limitation would apply in certain use cases and with respect to certain business activities.[141] For example, the Panel recommended that the CFPB consider options that would permit uses of data (including de-identified or anonymized data, as discussed below) for product maintenance or improvement, if appropriate consumer protections can be put in place.[142] The SBREFA Panel also recommended that the CFPB consider where it can give flexibility to third parties while still achieving its consumer protection objectives.[143]

The CFPB is proposing the examples in § 1033.421(c) to provide third parties with additional clarity on how the limitation standard would apply with respect to certain business activities. The CFPB requests feedback on whether the final rule should include other examples of business activities that are reasonably necessary to provide consumer requested products and services.

The CFPB also requests 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 CFPB requests 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 data, while requiring third parties to certify not to use covered data for certain higher-risk secondary uses. In addition, the CFPB requests feedback on whether the final rule should permit third parties to solicit a consumer's opt-

[141] *Id.* at 44–45.

[142] *Id.* at 44.

[143] *Id.* at 44–45.

in consent to engage in secondary uses with de-identified data, and if so, what de-identification standard the rule should provide.[144] The CFPB also requests 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 CFPB's proposed authorization disclosure is an appropriate vehicle for soliciting granular consumer choices about data use, such as through a secondary use opt-in mechanism. Finally, the CFPB requests 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.

Accuracy (§ 1033.421(d))

Proposed § 1033.421(d) would require 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 proposed § 1033.421(d), 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 commit to periodically reviewing its policies and procedures and updating them as appropriate to ensure their continued effectiveness. Proposed § 1033.421(d)(3) provides two elements that third parties should consider when developing their policies and procedures: (1) accepting covered data in the format required by § 1033.311(b), and (2) addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data. Finally, proposed § 1033.421(d)(4) states that indicia that a third party's policies and procedures are reasonable include whether the policies and procedures conform to a qualified industry standard regarding accuracy.

The CFPB has preliminarily determined that consumers would 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, would limit the effectiveness of the data access right fundamental to CFPA section 1033. Such inaccuracies would also impair the development of an innovative, competitive market for alternative consumer financial products and services. Third party accuracy requirements would also benefit third parties that rely on intermediaries to facilitate consumer-authorized access.

Proposed § 1033.421(d) would limit the scope of a third party's required policies and procedures to the accuracy of transmission—receiving covered data from a data provider and, if applicable, subsequently providing it to another third party. The CFPB has several reasons for proposing this scope. First, existing Federal law already protects consumers against some of the most harmful inaccuracies in the use of financial data. For example, FCRA imposes accuracy requirements on the information provided by consumer reporting agencies; Regulation E protects consumers against unauthorized electronic fund transfers and other errors; and Regulation Z protects consumers against certain billing and servicing errors.[145] Second, 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) would reflect this feedback. Finally, the CFPB understands that 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.

By requiring flexible standards rather than prescriptive rules, proposed § 1033.421(d) is designed to adapt to changing conditions and minimize the burden on third parties. Proposed § 1033.421(d)(1) would provide that a third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities. Proposed § 1033.421(d)(3) would offer elements that a third party should consider when designing its policies and procedures. Although reasonable policies and procedures would address many elements, the two identified in the proposal are especially relevant to an assessment of whether a third party's policies and procedures are reasonable. First, given the SBREFA feedback identifying transfer of data from a data provider as the primary source of inaccuracies, policies and procedures would likely be unreasonable if they failed to ensure that a third party could accept data in the format in which data providers made it available. And addressing information, such a dispute or notice of inaccuracy, from a consumer, data provider, or another third party is relevant to the reasonableness of a third party's policies and procedures because these other parties are likely to have information about whether data has been accurately transferred to or from the products or services they are using or providing. The implementation of these elements would vary according to a third party's size or market environment. For example, a data aggregator that supports a large number of additional third parties might require more extensive policies and procedures to reasonably ensure accuracy than a third party that acts only as a data recipient.

Proposed § 1033.421(d)(4) states that indicia that a third party's policies and procedures are reasonable include whether the policies and procedures conform to a qualified industry standard regarding accuracy. A qualified industry standard regarding accuracy is relevant to the reasonableness of a third party's policies and procedures because it reflects the openness, balance, consensus, transparency, and other requirements of proposed § 1033.141.

Flexible standards also facilitate consistency with existing accuracy requirements. For example, third parties might have obligations under existing law for investigating and responding to consumer disputes. By forgoing prescriptive dispute requirements, the proposal avoids conflicting with the format, substance, and timing requirements of the dispute provisions in other laws. The proposal's policies-and-procedures requirement would also allow third parties to leverage existing systems for addressing disputes to the extent that such disputes also relate to the transfer of covered data.

The CFPB seeks comment on proposed § 1033.421(d), including on whether any additional elements bearing on the reasonableness of a third party's policies and procedures regarding accuracy should be included.

Data Security (§ 1033.421(e))

Proposed § 1033.421(e)(1) would require third parties to certify to consumers that they will apply an information security program that

[144] For example, one standard suggested by SBREFA commenters, articulated in a 2012 FTC privacy report, and codified in several State laws describes de-identified information as data for which a business has (1) taken reasonable measures to ensure that the information cannot be linked to an individual; (2) publicly committed not to attempt to re-identify the information; and (3) contractually obligated any recipients not to attempt to re-identify the information. *See* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* at 20–21 (2012), *https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers;* Cal. Civ. Code section 1798.140(m); Colo. Rev. Stat. section 6–1–1303(11); Va. Code sections 59.1–575, 59.1–581; Utah Code Ann. 13–61–101(14).

[145] *See* 12 CFR part 1022; 12 CFR part 1005; 12 CFR part 1026.

satisfies the applicable rules issued pursuant to the GLBA (GLBA Safeguards Framework) to their systems for the collection, use, and retention of covered data. Proposed § 1033.421(e)(2) would require a third party that is not a GLBA financial institution to apply the information security program required by the FTC's GLBA Safeguards Rule (16 CFR part 314).

As explained in part IV.C above, covered data includes sensitive financial data that might expose consumers to fraud or identity theft if it were exposed. The GLBA Safeguards Framework provides a familiar risk-based process for addressing data security that allows for adaptation to changing technology and emerging threats. Therefore, the CFPB has preliminarily determined that the GLBA Safeguards Framework can be used by third parties to appropriately protect consumer-authorized financial data.

The SBREFA Panel recommended that the CFPB consider options for ensuring that consistent minimum data security standards apply to third parties and data providers, and several commenters echoed this recommendation.[146] Requiring third parties to certify that they follow the GLBA Safeguards Framework helps ensure consistency in protection as a 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, most likely the Interagency Guidelines Establishing Information Security Standards issued by the Federal functional regulators. However, a few commenters asserted that the FTC's Safeguards Rule may be insufficient because, unlike the Interagency Guidelines, it was not supported by regulator supervision. The CFPB understands this point but notes that the FTC has designed its rule to account for a different supervisory context. 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.[147]

Proposed § 1033.421(e)(1) would also limit burden on third parties and avoid duplicative regulation. As with data providers, third parties are already subject to data security requirements. The CFPB understands that all or most third parties that would access covered data through a developer interface are regulated by the GLBA Safeguards Framework, most commonly the FTC's Safeguards Rule.[148] As the CFPB discussed in a recent circular, inadequate data security can also constitute an unfair practice in violation of the CFPA.[149] However, the CFPA's unfairness prohibition articulates a general standard that is not specific to data security, and gaps in GLBA coverage might exist given the diversity of third parties that the proposal would cover. A few SBREFA commenters stated that they had observed third parties either denying or expressing uncertainty over their status as GLBA financial institutions. Requiring third parties that are not GLBA financial institutions to certify that they comply with the FTC's Safeguards Rule would remove any uncertainty and prevent any attempts to evade coverage.

Provision of Covered Data to Other Third Parties (§ 1033.421(f))

The CFPB is proposing in § 1033.421(f) to require the third party to certify that, before providing covered data to another third party, it will require the other third party by contract to comply with certain obligations.

In some circumstances, third parties that are authorized to access covered data from a data provider on behalf of a consumer may 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 has preliminarily determined that the consumer protections provided by the third party obligations in proposed § 1033.421 generally should continue to apply when the covered data are provided by the authorized third party to another third party. 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.

For this reason, proposed § 1033.421(f) would obligate the third party to certify that, before providing the covered data to another third party, it will require the other third party by contract to comply with certain third party obligations in proposed § 1033.421. Proposed § 1033.421(f) states 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 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) would not require the authorized third party to bind the other third party by contract to comply with all of the third party obligations in proposed § 1033.421. The CFPB has 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 requests 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 requests comment on which third party obligations in proposed § 1033.421 should be included in this approach.

Ensuring Consumers Are Informed (§ 1033.421(g))

The CFPB is proposing in § 1033.421(g) to require a third party to certify that it agrees to certain obligations designed to ensure that consumers are able to obtain information about the third party's access to their data.

As described above, to be authorized to access covered data on behalf of the consumer, a third party would be required to provide the consumer with an authorization disclosure.[150] The authorization disclosure would include, among other things, a brief description of the product or service that the

[146] SBREFA Panel Report at 44.

[147] 86 FR 70272, 70287 (Dec. 9, 2021).

[148] The CFPB is seeking comment in part IV.D about whether certain third parties, such as natural person third parties not covered by GLBA, should not be subject to the authorization procedures under proposed § 1033.401.

[149] Consumer Fin. Prot. Bureau, *Consumer Financial Protection Circular 2022–04* (Aug. 11, 2022), *https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/*.

[150] *See* proposed § 1033.401(a).

consumer requested and the categories of covered data the third party would access.[151] The CFPB has 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.

For this reason, under proposed § 1033.421(g)(1), a third party would be required to certify that it will provide the consumer with a copy of the consumer's authorization disclosure by delivering a copy to the consumer or making it available in a location that is readily accessible to the consumer, such as the third party's interface. The proposed rule specifies that, if the third party makes the authorization disclosure available in such a location, the third party also certifies that it will ensure it is accessible to the consumer until the third party's access to the consumer's data terminates. The CFPB seeks comment on whether this is the right time period.

In addition, the CFPB has 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 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.

For this reason, under proposed § 1033.421(g)(2), a third party would be required to certify that it will 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. 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 seeks 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.

The CFPB also has preliminarily determined that, at any time during the third party's access to the consumer's data, the consumer should be able to obtain certain information from the third party. For this reason, under proposed § 1033.421(g)(3), third parties would be required to certify that they will establish policies and procedures designed to ensure that, upon the consumer's request, the third party will provide certain information to the consumer.

Under this provision, the consumer would be able to obtain information about additional parties with which the covered data was shared and reasons for sharing the covered data.[152] The CFPB has 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 consumer would also be able to obtain information about the status of the third party's authorization.[153] Under the proposed rule, the third party would certify that it will limit its collection of data to what is reasonably necessary to provide the consumer's requested product or service. However, 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. The CFPB's proposal would enable consumers to obtain this information.

The consumer would also be able to obtain certain information that is similar to the information listed on the authorization disclosure: 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.[154] Some consumers may want to obtain this information, but rather than seeking out a copy of their authorization disclosure, they may simply contact the third party. These provisions would enable consumers to obtain this information in this manner. The CFPB has preliminarily determined that it would be appropriate to require the third party to certify that it will provide this information on request given that the third party originally provided this information on the authorization disclosure.

The CFPB seeks comment on whether the list in proposed § 1033.421(g)(3) should be modified, including whether additional categories of information should be added.

Revocation of Authorization (§ 1033.421(h))

Proposed § 1033.421(h) would contain third party obligations related to consumers' revocation of authorization for third parties to access their covered data. As described below, as a condition of being authorized to access covered data on a consumer's behalf, the third party must certify to: (1) provide the consumer with an easily accessible and operable revocation mechanism; (2) notify the data provider, data aggregator, and certain other third parties when a consumer revokes the third party's authorization; and (3) abide by certain limitations on collection, use, and retention of covered data when a consumer revokes the third party's authorization.

Proposed § 1033.421(h)(1) would require third parties to certify to provide the consumer with a mechanism to revoke the third party's authorization to access the consumer's covered data. Under proposed § 1033.421(h)(1), the third party would be required to certify that such revocation mechanism will be as easy to access and operate as the initial authorization. Proposed § 1033.421(h)(1) would also require the third party to certify that the consumer will not be subject to costs or penalties for revoking the third party's authorization.

In the SBREFA Outline, the CFPB described an approach in which third parties would certify to providing consumers with a simple way to revoke third party authorization to access data at any point.[155] In the SBREFA Outline, the CFPB defined revocation as a consumer withdrawing consent to third party data access that they previously authorized under the rule.[156] Commenters supported giving consumers the right to revoke third party consent at any time and made varying suggestions about the appropriate method for revocation. The following are some specific comments related to revocation: consumers should have the right to revoke consent in a manner that is consistent with initial consent; and revocation should be easy, readily accessible, clear, accessible via toggle on dashboard, free of cost/penalties, and/or salient. Many commenters supported the idea that third parties that receive revocation requests should notify the other parties of the request. The SBREFA Panel recommended that the CFPB explore

[151] *See id.* § 1033.411(b)(1) through (6) (content of the authorization disclosure).

[152] *See id.* § 1033.421(g)(3)(iii) and (iv).

[153] *See id.* § 1033.421(g)(3)(v).

[154] *See id.* § 1033.421(g)(3)(i), (ii), and (vi).

[155] SBREFA Outline at 42.

[156] *Id.*

options that enable consumers to revoke third party access and clarify the kind of revocation mechanisms third parties would be required to provide to consumers.[157] The SBREFA Panel also recommended that the CFPB continue to consider how revocation requirements could be designed to reduce impacts on third parties.[158]

The CFPB has 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. For this reason, the CFPB has preliminarily determined that consumers need sufficient, clear opportunities to revoke their consents to third party access to covered data under this proposed rule. As such, proposed § 1033.421(h)(3) is designed to achieve the goal of ensuring consumers can provide meaningful authorization to third party data access and easily and effectively revoke that authorization whenever they choose. The CFPB has preliminarily determined that revocation should be as easy as the initial authorization to ensure third parties do not bury the revocation mechanism or otherwise obfuscate consumers' ability to utilize it.

Additionally, for revocation of authorization to be free of cost or penalties to the consumer, the CFPB has preliminarily determined that 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. 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 proposed § 1033.421(h)(1), third parties must allow consumers to revoke consent to data access for a particular product or service and maintain consent to data access for any others.

Further, proposed § 1033.421(h)(2) would require the third party to certify that it will notify the data provider, any data aggregator, and other third parties to whom the third party has provided the consumer's covered data when the third party receives a revocation request from the consumer. As noted above, in some circumstances, third parties that are authorized to access covered data from a data provider on behalf of a consumer may want to share that data with another third party. The CFPB is proposing in § 1033.421(f) to obligate the third party to certify that, before providing covered data to another third party, it will require the other third party by contract to comply with certain third party obligations in proposed § 1033.421. In addition, proposed § 1033.431(c), discussed below, would require that, when a third party uses a data aggregator to assist with accessing covered data on behalf of a consumer, the data aggregator certify to the consumer that it agrees to the conditions on accessing the consumer's data in proposed § 1033.421(a) through (f) and (h)(3). The CFPB is proposing in § 1033.421(h)(2) to require authorized third parties to 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 is also proposing 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.

Finally, proposed § 1033.421(h)(3) would require the third party to certify that, upon receipt of a consumer's revocation request or notice of a revocation request pursuant to proposed § 1033.321(3), the third party will (1) no longer collect covered data pursuant to the most recent authorization, and (2) no longer user 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).

Proposed § 1033.421(h)(3)(i) specifies the effect of a consumer's revocation request on the third party's collection of covered data. As noted above, the CFPB is proposing in § 1033.421(h)(1) to require third parties to certify to provide consumers with a mechanism by which they can revoke the third party's authorization. Consistent with that provision, proposed § 1033.421(h)(3)(i) specifies that, once a consumer requests revocation, the third party may no longer collect covered data pursuant to the consumer's authorization.

Proposed § 1033.421(h)(3)(ii) specifies the effect of a consumer's revocation request on the third party's use and retention of covered data collected prior to that request. Consistent with the general limitation in proposed 1033.421(a), proposed § 1033.421(h)(3)(ii) specifies that, when a consumer requests revocation of third party authorization, 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.

This provision mirrors proposed § 1033.421(b)(4)(ii), which addresses the effects of the maximum durational period on use and retention of previously collected data. As where a consumer does not reauthorize third party access before the maximum durational period expires, revocation of the consumer's existing authorization to access, all other things being equal, covered data indicates that such authorization no longer supports use or retention of data collected under its terms. In the normal course, therefore, application of the general standard in proposed § 1033.421(a) will call for the third party to stop using and retaining data collected pursuant to that authorization. However, as noted above with respect to proposed § 1033.421(b)(4)(ii), exceptional circumstances may justify continued use and or retention of some or all such data under that standard, even as new collection, use, and retention stops. For example, a subpoena could require the retention, post-revocation, of specific data collected pre-revocation; meeting such legal requirements can continue to remain reasonably necessary even if only in connection with providing the product prior to revocation. Similarly, the consumer could provide a clear, affirmative indication that they want to continue to use the product, post-revocation, in a manner supported by the use and retention of data collected prior to revocation. In that context, use and retention of some or all of the data could meet the general standard in proposed § 1033.421(b)(4)(ii) even as the consumer no longer makes use of the product in any manner that would require continued data collection.

The CFPB has preliminarily determined that proposed § 1033.403(h)(3)(ii), like proposed § 1033.421(b)(4)(ii), 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 standard in proposed § 1033.421(a), while ensuring that consumer data are not used and retained, post-revocation, in a manner that does not properly reflect the control afforded the consumer under that same general standard. The CFPB seeks comment about these circumstances and whether, following revocation, additional protections for consumers or flexibilities for third parties are warranted.

[157] SBREFA Panel Report at 45.

[158] *Id.*

5. Use of Data Aggregator (§ 1033.431)

The CFPB is proposing to adopt certain requirements for the third party authorization procedures when a third party will use 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. Proposed § 1033.431 would assign certain responsibilities for the authorization procedures and impose certain conditions on the third party and the data aggregator.

Responsibility for Authorization Procedures

Proposed § 1033.431(a) would 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 provides that the third party remains responsible for compliance with the third party authorization procedures and that data aggregators must comply with the data aggregator certification requirements in proposed § 1033.431(c).

The CFPB has preliminarily determined that the third party should be responsible for compliance with the third party authorization procedures. 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 has preliminarily determined that it is appropriate for the third party to have responsibility for compliance with the third party authorization procedures.

The CFPB recognizes, 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 is proposing to allow, but not require, a data aggregator to perform the authorization procedures on behalf of a third party. 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.

The CFPB considered proposing a requirement that the data aggregator be responsible for the authorization procedures. However, a consumer may not be familiar with the data aggregator or the role that the data aggregator may play in accessing covered data. The CFPB also considered allowing data aggregators or third parties to decide which party would be responsible for compliance with the authorization procedures or allowing or requiring both third parties and data aggregators to perform the authorization procedures but has preliminarily determined that the clearest and least confusing approach for consumers would be to have the third party seeking access to covered data be responsible for compliance with the authorization procedures.

Disclosure of the Name of the Aggregator

Proposed § 1033.431(b) would 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. Unlike other downstream parties that may access a consumer's covered data after they have 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 a data aggregator performs the authorization procedures on behalf of a third party. Therefore, the CFPB has 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 CFPB seeks comment on any obstacles to including a data aggregator's name in the authorization disclosure.

Aggregator Certification

Proposed § 1033.431(c) would require that, when a third party uses 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 § 1033.421(h)(3) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data.

The CFPB is 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. If data aggregators were not required to agree to the conditions in proposed § 1033.421, there could be a significant gap in the protections afforded to consumers under the proposed rule. In addition, as with the third party's certification statement,[159] the CFPB wants the consumer to receive a clear statement of the conditions that the data aggregator must follow, and this certification would be helpful in allowing a consumer and the CFPB and other regulators to enforce these obligations if the data aggregator breaches these obligations. 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.

Proposed § 1033.431(c) provides that, for this aggregator certification requirement to be satisfied, either (1) the third party must include this aggregator certification in the authorization disclosure it provides the consumer, or (2) the data aggregator must provide to the consumer a separate certification. 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 third party obligations described in proposed § 1033.421. The 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 seeks 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.

6. Policies and Procedures for Third Party Record Retention (§ 1033.441)

The CFPB is proposing in § 1033.441, generally, to require a third party that is

[159] *See* discussion of proposed § 1033.401(b).

a covered person or service provider, as defined in 12 U.S.C. 5481(6) and (26), to establish and maintain policies and procedures reasonably designed to ensure retention of records that evidence compliance with proposed subpart D. Proposed § 1033.441 would be authorized under CFPA section 1022(b)(1) because it would enable the CFPB and others to evaluate a third party's compliance with proposed subpart D and would prevent evasion. To the extent that proposed § 1033.441 would apply to CFPB-supervised nondepository covered persons, it would additionally be authorized by CFPA section 1024(b)(7) because it would facilitate supervision of such persons and enable the CFPB to assess and detect risks to consumers.

Proposed § 1033.441 generally would require third parties to establish and maintain policies and procedures to retain records for a reasonable period, not less than three years after a third party obtains the consumer's most recent authorization under § 1033.401(a). Proposed § 1033.441(b) bases 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 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 requests 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. Proposed § 1033.441 sets forth a flexible approach by establishing a minimum retention period and by not exhaustively specifying categories of records, which likely would be infeasible given the wide range of activities subject to proposed subpart D. Under proposed § 1033.441(c), a third party would have flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities. 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) identifies examples of records that would need to be retained. Further, proposed § 1033.441(d) would require a third party to commit to periodically reviewing its policies and procedures and updating them as appropriate to ensure their continued effectiveness. 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.[160] The CFPB requests comment on whether the final rule should identify other examples of records to be retained.

As described above related to § 1033.421(b) and (h), the CFPB is proposing to require a third party to no longer retain covered data following a maximum durational period ending or upon a consumer's request for revocation, unless retention remains reasonably necessary. Proposed § 1033.421(b)(4) and (h)(3) are not designed to impact the requirement of proposed § 1033.441 for a third party to maintain policies and procedures to retain records for a reasonable period proposed in § 1033.441, as proposed § 1033.441 covers records that evidence compliance with proposed subpart D. In contrast, § 1033.421(b)(4) and (h)(3) cover data collected from data providers to provide a requested product or service. The CFPB seeks comment on whether additional guidance might be needed on the potential intersections of the record retention requirements in proposed § 1033.441 and limitations on retention in § 1033.421(b)(4) and (h)(3).

12 CFR Part 1001

Providing Financial Data Processing Products or Services (§ 1001.2(b))

The proposed rule would add § 1001.2(b) to part 1001 to define 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 CFPB preliminarily concludes that the activities in proposed § 1001.2(b) are already within scope of the CFPA's definition of financial product or service. Nevertheless, the CFPB is proposing to use its rulemaking authority to provide even greater certainty on this issue.

Under CFPA section 1002(15)(A)(xi)(II), the CFPB may issue a regulation to define as a financial product or service, for carrying out the objectives of CFPA section 1033, ''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 proposing § 1001.2(b) pursuant to this authority.

As noted above, the CFPB's preliminary view is that the activities in proposed § 1001.2(b) are already 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, including where the financial data are processed in connection with other financial or non-financial products or services. 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.[161]

However, the CFPB is proposing to use its rulemaking authority to provide even greater certainty on this issue. 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, this proposed rule has the potential to greatly expand access to personal financial data and subject such data to a wider variety of data processing activities. The CFPB is thus proposing to add to the definition of financial product or service the category of ''providing data processing product or services'' to ensure that activities involving consumers' potentially

[160] SBREFA Panel Report at 45.

[161] 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).

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.[162] The proposed definition includes examples to illustrate the breadth of activities that fall within the term financial data processing. The reference to financial data processing in connection with another product or service, as discussed above with respect to CFPA section 1002(15)(A)(vii), comprises both financial and non-financial products or services.

The CFPB preliminarily finds that proposed § 1001.2(b) meets the two factors set forth in CFPA section 1002(15)(A)(xi)(II). First, the activities in proposed § 1001.2(b) are permissible for financial holding companies under the Federal Reserve Board's Regulation Y and for national banks under OCC regulations. 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.[163]

Second, processing of personal financial information has, or is likely to have, a material impact on consumers. As already discussed 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 this 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, to the extent they are not already included within the definition of a financial product or service under CFPA section 1002(15)(A)(vii), would raise the same type of consumer protection concerns as activities that do fall within this definition.

Proposed § 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 12 U.S.C. 5481(15)(A)(vii)(I) or (II), is not a covered person. 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 proscribed processing activities. CFPA section 1002(15)(A)(vii)(I) excludes as covered persons certain merchants, retailers or sellers of non-financial products or services that are solely engaged in certain activities related to initiating payment instructions, whereas CFPA section 1002(15)(A)(vii)(II) excludes persons that solely provide access to a host server for websites. The CFPB proposes to parallel these exclusions in proposed § 1001.2(b).

V. Proposed Effective Date

The CFPB proposes that the establishment of part 1033 and the amendment to part 1001 shall take effect 60 days after the date of the final rule's publication in the **Federal Register**. In the case of part 1033, proposed § 1033.121 provides for staggered compliance dates for data providers. In the case of the amendment to part 1001, the CFPB has preliminarily determined that the activities covered by the amendment are already within the scope of the CFPA's definition of financial product or service, as explained in part IV, and so no compliance date is necessary.

VI. CFPA Section 1022(b) Analysis

The CFPB is considering the potential benefits, costs, and impacts of the proposed rule. The CFPB requests comment on the analysis presented below, as well as submissions of additional data that could inform its consideration of the benefits, costs, and impacts of the proposed rule.

A. Statement of Need

In section 1033 of the CFPA, Congress directed the CFPB to adopt regulations governing consumers' data access rights. The CFPB is issuing this proposed rule primarily to begin implementing the CFPA section 1033 mandate, although the CFPB is also relying on other CFPA authorities for specific aspects of the proposed rule.

Because the primary purpose of this proposed 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 proposed 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 rights and current practices, and describes the overall goals of the proposed rule in closing those gaps. The remainder of the CFPA section 1022(b) analysis discusses the benefits, costs, and impacts of the specific provisions to address these gaps, and potential alternatives.

Consumers should have control over their financial data, including accessing their data when desired, and controlling who else can access their data and for what purposes. When consumers access their financial data today, they often do not have this control. Consumer financial data are often accessed through methods that raise data security and privacy risks and consumers have little to no control over how the data are used by third parties that have access to it. In addition, there is a lack of secure, 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 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 data formats used. This creates inefficiencies for market participants, as every connection between a third party and a data provider requires many detailed terms and conditions to be negotiated. This often entails substantial levels of cost. This proposed rule aims to (1) expand access for consumers 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 greater competition, and support the development of beneficial products and services.

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,[164] as well as data

[162] 12 U.S.C. 5531, 5536.

[163] 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).

[164] For information about the data collected in the Provider Collection and Aggregator Collection, respectively, *see 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 Aug. 28, 2023). Because data

Continued

obtained from other regulatory agencies [165] and publicly available sources.[166]

In 2016, the CFPB released and received comments on a Request for Information 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 2022, the CFPB convened a SBREFA Panel to gather input from small businesses and in 2023 the Panel issued the SBREFA Panel Report.[167] The CFPB also solicited and received comments from other industry participants on the SBREFA Outline.[168] In addition to these sources of information, these impact analyses are informed by consultations with other regulatory agencies, industry, and researchers. The CFPB's outreach is described in detail in part II.

For the types of financial data and access generally covered by this proposed 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; as well as 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.[169] The CFPB seeks additional information or data that could refine these estimates.

For data on the number and characteristics of covered depository institutions, the CFPB relies on data from FFIEC and NCUA Call Reports.[170] 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 FDIC- or NCUA-insured deposit accounts, which are an imperfect, but nonetheless the best available proxy for the number of covered financial 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 proposal. 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.[171]

To estimate costs to small entities of the provisions, the CFPB relies on information gathered from the SBREFA process. This includes both written feedback submitted by small entity representatives and the discussions at the SBREFA Panel summarized in the SBREFA Panel Report.[172]

C. Coverage of the Proposed Rule

Part VII.B.3 provides a discussion of the number and types of entities affected by the proposed rule.

D. Baseline for Consideration of Costs and Benefits

In evaluating the proposal'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 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, *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.[173]

In total, the CFPB estimates that there were between 50 billion and 100 billion total consumer-authorized access attempts in 2022.[174] Usage has grown substantially over the last four years, as the annual number of consumer-authorized access attempts approximately doubled from 2019 to 2022.

---

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 similar third parties.

[165] In particular, these include entity-level FFIEC and NCUA data on characteristics of depository institutions.

[166] 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.

[167] 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.*

[168] Consumer Fin. Prot. Bureau, *CFPB Kicks Off Personal Financial Data Rights Rulemaking* (Oct. 7, 2022), *https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-personal-financial-data-rights-rulemaking/.*

[169] 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.*

[170] *See* Fed. Fin. Insts. Examination Council, *Central Data Repository's Public Data Distribution, https://cdr.ffiec.gov/* (last visited Sept. 12, 2023), 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. 7, 2023).

[171] *See* Nat'l Credit Union Admin., *CUOnline, https://ncua.gov/regulation-supervision/regulatory-reporting/cuonline* (last visited Oct. 5, 2023).

[172] 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.*

[173] 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.

[174] 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.

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, currently most access attempts 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 has grown 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 has declined from 80 percent in 2019 to 50 percent in 2022. Credential-based APIs have seen 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. The CFPB understands that 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. The CFPB estimates that at the end of 2022, between 5 and 10 percent of all data providers offered credential-free APIs, up from less than 1 percent in 2021. The CFPB understands that 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.[175] While adoption is relatively high for the largest depository data providers, the CFPB estimates that only between 10 and 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, of course, uncertain. However, based on the data and market trends available, the CFPB makes the following assumptions for the baseline in this impact analysis. First, most of the very largest data providers have adopted or likely would in the near future adopt credential-free APIs, which would meet many—but possibly not all—requirements contained in the proposal. Awareness of CFPA section 1033 may have contributed to these outcomes, 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. 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 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.

The CFPB understands that all or most data providers and third parties seeking to access consumer-authorized information are subject to the GLBA, specifically either the FTC's Safeguards Rule or the Federal functional regulators' Interagency Guidelines. Additionally, third parties that operate in one of the 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. As described in part I.E.2, some third parties have obligations under the FCRA. 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 proposed rule, though individual company systems or policies will depend on the size, location, practices, and other circumstances of each third party.

The impact analysis generally includes the major elements of costs to firms of complying with the proposed 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 proposed rule. For example, where data providers have adopted some form of credential-free third party access under the baseline, the analysis discusses how the proposal would impact the terms, costs, and features of those interfaces.

Finally, in the context of direct access, all non-exempt data providers offer some digital banking interface and the CFPB assumes for its baseline that these interfaces typically provide all or nearly all data fields required to be made available by the provisions. The analysis considers how the provisions would impact the costs and features of those digital banking interfaces. Those covered entities that do not offer any form of digital banking would be exempt from the proposed rule's requirements.

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.

Individual provisions of the proposed rule may have costs for some groups and benefits for others. And some provisions interact with one another, preventing them from being analyzed in isolation. As a result, the discussion of costs for one group will not provide the net impacts of a particular provision or of the proposed rule as a whole. The net impacts depend on the combination of costs and benefits across data providers, third parties, and consumers.

1. Costs to Covered Persons

Costs to Data Providers

As a result of the proposed rule, data providers may face increased costs

[175] For example, *see* Press Release, *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.*

related to maintaining consumer interfaces and establishing and maintaining developer interfaces, including modifying their existing systems to comply with the proposed rule. The CFPB expects the largest costs to data providers to come from establishing and maintaining compliant developer interfaces. Covered data providers would also incur costs related to developing and implementing policies and procedures governing those systems. The proposed 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.

Maintaining an Interface for Direct Consumer Access

The proposed rule would require data providers to make covered data available through consumer interfaces and to allow consumers to export the information in machine-readable formats. Data providers that do not offer a consumer interface would be exempt from the requirements of the proposed rule. 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.[176] Based on this feedback, the proposed rule would cover 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 proposed 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 account opening disclosures. The CFPB does not have sufficient data to quantify the levels of these costs. The CFPB requests data or information on whether any of the required data fields are not provided through consumer interfaces, as well as on the costs of adding such fields to consumer interfaces.

Establishing and Maintaining an Interface for Third Party Access

The proposed rule would require data providers to establish and maintain a compliant developer interface. Although many data providers already maintain developer interfaces, others would need to establish new interfaces, likely integrated with existing infrastructure that supports their consumer interfaces. The CFPB expects that the costs of modifying an existing developer interface to ensure compliance with the proposed rule would depend on the scope and nature of the necessary modifications but would generally be lower than the cost of establishing a new interface.[177]

In general, data providers must either contract with a vendor for their developer interfaces or develop and maintain such interfaces in-house. The analysis below estimates compliance costs under these two approaches. Some data providers may comply with the proposed rule through a combination of 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 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 their developer interface. 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.[178] Based on comments received during the SBREFA process and market research, the CFPB understands that other core banking providers charge flat monthly fees or per-account fees.[179] The CFPB understands that these fees vary but generally estimates that fees can be up to $24 per account per year.[180] The CFPB requests information related to the developer interfaces offered by core banking providers and other vendors and how such interfaces are priced.

Data providers taking this approach will generally have minimal upfront costs to deploy a developer interface. However, some data providers use service providers that do not currently offer a developer interface. 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. 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.[181] 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,

[176] SBREFA Panel Report at 24.

[177] 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.

[178] For example, *see* Jack Henry & Assocs., Inc., *Secure Data Connection: take back control of account connection, https://banno.com/data-aggregators/* (last visited Aug. 7, 2023).

[179] SBREFA Panel Report at 37.

[180] *Id.* at 38.

[181] *See* 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 CFPB expects that the true share of 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 their interfaces 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 small depository data providers, given that they have the latest compliance date.

Under the in-house approach, data providers would primarily employ software developers or similar staff to build and operate their developer interfaces. The estimates below are based on a fully in-house development 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 provided here.

The CFPB expects that most data providers that already develop and maintain consumer interfaces in-house would also develop and maintain their developer interface in-house.[182] In the SBREFA Outline, the CFPB estimated that developing a compliant developer interface 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 $216,000 to $432,000, updated to $237,000 to $475,000 based on more recent labor cost data.[183] 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 estimates that nondepository data providers may require only 480 hours of work by software developers at a total cost of $44,000.[184] In addition to these upfront costs, the CFPB estimates that data providers taking the in-house approach incur ongoing costs of $3 to $5 per account per year to maintain a compliant developer interface in-house, based on evidence from the Provider Collection described below.

During the SBREFA Panel meetings, data provider small entity representatives stated that establishing a compliant developer interface would require developing multiple internal APIs because their data are stored on three to eight separate information technology systems, most of which are not currently connected to their core banking system.[185] Depository small entity representatives estimated that each of these internal APIs could cost approximately $60,000 in upfront staffing costs and $20,000 in ongoing technology costs.[186] Nondepository small entity representatives estimated lower upfront staffing costs, of 240 to 480 hours, or $22,000 to $44,000. Although nondepository small entity representatives did not estimate ongoing technology costs, the CFPB expects these costs will generally also be smaller than costs for depository small entity representatives.[187] Based on this feedback, the proposed rule would require a more limited set of information to be provided, relative to those under consideration in the SBREFA Outline. The proposed rule's approach should significantly reduce the need for new internal APIs, particularly since the categories of information included in the proposed rule largely align with those available through consumer interfaces at most data providers.

Some small entity representatives stated that the CFPB's original estimate in the SBREFA Outline of $216,000 to $432,000 was too low, and one small entity representative estimated that the cost was likely to be above $500,000.[188] However, changes in the proposed rule should significantly reduce the need for new internal APIs, which was a primary component of these higher estimated costs. Therefore, the CFPB estimates a total upfront cost of $250,000 to $500,000 for small depository data providers that choose to build their developer interface in-house. Small nondepository data providers are likely to have somewhat smaller upfront costs. Based on small entity representative feedback, the CFPB estimates that small data providers choosing to build their developer interface in-house will incur ongoing annual technology costs of $20,000 as well as ongoing staffing costs of $45,000 to $91,000.[189]

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

[182] As discussed below, data providers have generally indicated that the resources required to maintain a developer interface in-house are a small fraction of the resources required for consumer interfaces. Therefore, the CFPB expects that data providers that have already invested in the capacity to operate a consumer interface in-house will take a similar approach to developer interfaces. 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 obtain developer interfaces from service providers.

[183] This estimate was derived from BLS data showing a mean hourly wage for software developers of $63.91. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $91.30 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

[184] 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.

[185] SBREFA Panel Report at 37.

[186] *Id.*

[187] One data provider small entity representative that recently implemented an API explained that it and its vendors had spent approximately 50–60 hours understanding the requirements and planning, 50–60 hours creating the database, 80 hours prototyping for optimization and security, and 40 hours testing and documenting, or roughly 220–240 hours to develop and implement the API, in addition to ongoing hardware and cloud hosting expenses. Two nondepository data provider small entity representatives estimated that it would take one internal staff member approximately 12 weeks to comply with the proposed rule. Other small entity representatives stated that implementation would likely be less difficult for nondepository data providers because they do not have as many vendors or separate information technology systems.

[188] SBREFA Panel Report at 37–38.

[189] 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 2022 shows a mean hourly wage for software developers of $63.91. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $91.30 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

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.[190] 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 proposed 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 CFPB requests additional data on the cost of developing and maintaining compliant developer interfaces compared to contracting with a service provider.

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 proposed 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 provide a precise estimate of the cost of bringing such systems into compliance with the proposed rule. However, that cost would generally be a fraction of the cost of developing and maintaining a new interface, as described above.

The CFPB seeks comment or additional data on the extent to which existing developer interfaces will need to be modified to meet the requirements of the proposed rule and the cost of required modifications relative to the cost of establishing a new compliant developer interface.

Developing and Implementing Policies and Procedures

The proposed rule would include disclosure and recordkeeping requirements for all covered data providers related to consumer-authorized data access. The proposed rule would require data providers to tally and disclose the number of proper responses divided by the total number of queries to their developer interface (the ''response rate'') 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 $7,300 per data provider.[191] 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 proposed rule would require 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 proposed rule would also require 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 developer interface is communicated to the third party. The requirements to inform third parties when and why access was not permitted would likely be 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 likely 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 implementing a compliant developer interface, as described above. The CFPB has previously estimated that developing policies and procedures to comply with a rule of similar complexity would require a one-time cost of $2,500 to $4,300 per data provider, as well as a one-time cost of $3,000 to $7,600 for a legal and compliance review.[192] Therefore, the CFPB estimates a total one-time cost of developing and implementing policies and procedures as required by the proposed rule of $5,500 to $11,900 per data provider.

Indirect Costs

In addition to the direct costs described above, data providers are likely to incur indirect costs as a result of the proposed rule. The CFPB expects costs related to negotiating additional agreements with 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

[190] 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.

[191] This estimate was derived from BLS data showing a mean hourly wage for software developers of $63.91. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $91.30 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

[192] 86 FR 56356, 56556 (Oct. 8, 2021).

competition and enabling new products and services.

Increased Number of Agreements Between Data Providers and Third Parties

The proposed rule generally would require data providers to grant access to their developer interface, except for reasonable denials related to risk management or insufficient information. Although the proposed rule does not require formal data access agreements, the CFPB expects the proposed rule to lead to more third parties requesting and being granted access to data providers' developer interfaces relative to the baseline and that this is likely to require data providers to negotiate more agreements with third parties. In the Aggregator Collection responses, 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 proposed rule relative to the baseline because many features of data access agreements would be regulated by the proposed rule and not subject to negotiation, including requirements for interface reliability, 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 proposed rule nearly all data providers will use standardized agreements and the costs of establishing data access will generally be limited to ensuring third party risk management standards are satisfied and reviewing the agreements. The CFPB expects that this process will require 80 staff hours on average, representing approximately $6,800.[193] These costs may be further reduced if industry accreditations or standards develop which streamline data providers' required efforts on third party risk management. While some data providers and third parties may choose to negotiate customized data access agreements, they will generally only do so when the perceived benefits exceed the costs described here. Because the choice to negotiate a costly but more customized data access agreement is a business decision not required by the proposed rule, the additional costs of doing so are outside the scope of this analysis.

The total cost of negotiating additional agreements will depend on the difference between the number of agreements that would be negotiated under the baseline and the number that would be negotiated under the proposed rule. Because the consumer-authorized data system is developing rapidly, it is not possible to precisely estimate the number of additional connections that would be caused by the proposed rule. However, in the near term, the CFPB anticipates that most data providers will continue to offer third parties access to consumer-authorized data through specialized intermediaries, as they would have under the baseline. As a result, the CFPB expects that, on average, large data providers will need to negotiate 10 or fewer additional data access agreements in the years immediately following implementation of the proposed rule, at a maximum cost of $68,000 per large data provider. In contrast, smaller entities are likely to rely on core banking providers or other vendors to negotiate aspects of the agreements on their behalf at minimal incremental cost. Over time, data providers are likely to negotiate additional data access agreements due to entry by new third parties and other changes in the market.[194] The CFPB requests comment on how the proposed rule is likely to change both the cost of establishing data access agreements and the number of data access agreements negotiated by data providers.

Prohibition on Fees for Access

The proposed rule would not permit data providers to charge fees for the required interfaces or for access to covered data through their interfaces. To the extent that data providers are currently charging such fees, the proposed 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 interface of sufficient quality sufficiently quickly. While rare in the current market, the proposed rule would eliminate such fees that may 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 to their interfaces and that the total cost to data providers of eliminating such charges would be minimal.

More Frequent Access—Third Parties Allowed To Make More Frequent Data Queries

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 understands that data providers cap the number of data requests per day per connection. The proposed rule would generally 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. All else equal, this is likely to increase total data requests and may therefore increase digital infrastructure costs for covered data providers relative to baseline.[195] This increase is likely to be larger for data providers with more restrictive access caps at baseline. The CFPB expects that for most data providers, the 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

[193] This estimate was derived from BLS data showing a mean hourly wage for compliance officers ($37.01), general and operations managers ($59.07), lawyers ($78.74), and software developers ($63.91), for an average hourly wage of $59.68. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to an $85.26 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

[194] For example, the proposed rule aims to accelerate the development and adoption of qualified industry 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.

[195] As discussed in the *Benefits to data providers* section, 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.

per request than requests through a developer interface. A small number of large data providers have already restricted screen scraping and may experience net increases in developer interface traffic. In general, the CFPB expects that incremental costs from increased data requests are likely to be minimal on a per-account basis. The CFPB requests data or other information that would inform its estimates of the cost of additional data requests through a developer interface.

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 proposed rule would 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 proposed 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 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 *Benefits to Consumers* section.

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 CFPB requests additional data or information that would inform this analysis.

The proposed 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 opt in to such services, or how the availability of such services would impact individual firms or industries. The CFPB requests any additional data or information that would inform its analysis of this impact on data providers.

Costs to Third Parties

Third parties would 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 proposed rule may impose further costs on third parties through the transition away from screen scraping access and restrictions on data use and retention. Potential effects of the new financial data processing products or services definition are also discussed.

Implementing Mechanisms for Revocation of Authorization

The proposed rule would require third parties to establish and maintain systems that could receive data access revocation requests, track duration-limited authorizations, and delete data when required due to revoked authorizations, lapsed authorizations, or because retaining the data is no longer reasonably necessary. Third parties would also need to retain records as required by the proposed 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),[196] which requires that businesses delete consumer personal data upon consumer request. These third parties would likely need to modify their systems, incorporate authorization duration limits, and process more revocation requests, but they would likely have lower costs than third parties that must establish such a system from scratch. The CFPB estimated in the SBREFA Panel Report 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.[197]

As described in the SBREFA Panel Report, several small entity representatives provided cost estimates of implementing deletion requirements. At the low end, one third party small entity representative that had implemented deidentification and deletion systems stated that it took between 240 and 480 hours,[198] 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 for information deletion would take 1,000 hours. If a third party chose not to establish a system to implement the deletion requirements of the proposed rule and instead chose to manually delete data, the CFPB understands that the time cost would be substantially

[196] Cal. Civ. Code section 1798.198(a) (2018).

[197] 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.*

[198] 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.

higher: one third party small entity representative explained that, as an organization of fewer than 50 people, complying with a single deletion request could require 480 hours. Based on this feedback, the CFPB estimates that the cost of implementing deletion requirements would be between $21,900 and $91,300.[199] The CFPB expects that the cost would be lower for third parties that already comply with existing data privacy laws. The CFPB requests additional data or other information to further refine this estimate. Third parties that do not retain any consumer-authorized data would be unaffected by these requirements.

Annual Reauthorization Process

The proposed rule would limit the duration of third party collection of covered data to no more than one year after a consumer's most recent authorization. Third parties would 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 the new authorization would have the same legal requirements as the first authorization, most of its implementation costs would be captured by the costs described above for the initial authorization and 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 requirements may limit the quality 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. Any gaps in the third party's collection of consumer data would likely be filled once it obtains the new authorization, 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 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. Reauthorization requirements created frictions for third parties in the United Kingdom's open banking regime after the implementation of a 90-day reauthorization requirement. One UK 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.[200] These attrition rates may be different than those expected under the proposed rule because, on the one hand, a 90-day reauthorization requirement is more burdensome than an annual reauthorization requirement, but on the other hand, more consumers may still be actively using a product or service after 90 days than after one year and so may be more likely to reauthorize access. 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 customer 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 proposed rule would require 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 proposed rule would require the data aggregator to make its own certification statement to the consumer, though both the aggregator and third party certifications would be permitted to be made in the same disclosure. The CFPB expects that, in many cases in the market today, data aggregators would provide the required authorization disclosure and 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, 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.[201] The CFPB estimates that this would result in a one-time cost for a third party of $91,300. 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 $2,700 and $3,700.[202]

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 CFPB anticipates that this will be the case under the proposed rule. The CFPB does not have data to estimate these costs. However, because data aggregators' 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.

[199] 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 $63.91. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $91.30 estimate for total hourly compensation.

[200] *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.*

[201] 82 FR 54472, 54823 (Nov. 17, 2017).

[202] This estimate was derived from BLS data showing a mean hourly wage for software developers of $63.91. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $91.30 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

Record Retention

The CFPB understands that many third parties already retain records related to consumer data access requests. The proposed rule would require third parties to retain records that demonstrate compliance with the proposed rule, including a copy of the authorization disclosure and, if a data aggregator accessed consumer-authorized data, a copy of the certification statement. The costs of satisfying these requirements would be captured by the one-time costs to implement the revocation, use, and retention requirements. The three-year record retention requirement of the proposed rule would impose limited additional electronic storage costs.

Policies and Procedures

To implement the requirements of the proposed rule, third parties would need to develop and maintain policies and procedures in several distinct areas to ensure compliance with the proposed rule. These include (1) applying existing information security programs to their systems for the collection, use, and retention of covered data, (2) ensuring the accuracy of the information that they collect, (3) governing the limits on collection, use, and retention of consumer-authorized information, and (4) record retention requirements. The CFPB understands that all or 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 would have lower costs for developing and maintaining similar requirements of the proposed 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 $4,300 to develop new policies and procedures and a one-time cost of $3,900 for a legal/compliance review.[203] Assuming comparable costs for the requirements of the proposed rule yields a total cost of roughly $8,200 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.[204]

Transition Away From Screen Scraping

The CFPB expects that third parties may face indirect costs from the transition away from screen scraping under the proposed rule. 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 has declined by approximately one-third since 2019. The CFPB expects that screen scraping would continue to decline for non-covered financial products as data providers and third parties generally transition to developer interfaces for third parties. The CFPB expects that third parties would no longer use screen scraping to access covered financial data once data providers have compliant interfaces for third parties. While the CFPB expects data access volumes and the number of connections between third parties and data providers to increase as a result of the proposed rule, relative to the baseline third parties may incur additional costs related to contracting with data providers, as well as costs related to demonstrating to data providers the sufficiency of their risk management practices.

In the SBREFA process, multiple small entity representatives expressed that the transition away from screen scraping would limit data accessibility. The proposed rule would not apply to non-covered data. Relative to the baseline, the CFPB does not expect the transition away from screen scraping to negatively impact data availability. The CFPB requests 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.

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 would be reduced under the proposed rule because the proposed rule would improve the reliability of data access systems, but in the current system at least one small entity representative stated that customers lose access to the small entity representative's services when access to data providers' interfaces is unavailable. 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 and reliability of interfaces for third parties. The CFPB requests data or evidence to quantify these potential effects.

Third parties that previously accessed covered data through screen scraping without negotiating the terms of their access with data providers would negotiate these terms under the proposed rule. The CFPB expects that many of these negotiations would occur between data aggregators and data providers, though some negotiations would occur between authorized third parties that do not contract with data aggregators and data providers. As described in the *Costs to Data Providers* section, the CFPB estimates that the cost of negotiations between data aggregators and data providers would be $6,800. One data aggregator suggested in its response to the Aggregator Collection that the cost of negotiation could fall by 80 percent under the proposed rule, as 60 percent of work hours for employees involved in negotiations are spent on topics that would be regulated by the proposed rule and nonnegotiable, and another 20 percent of work hours are spent on topics that would be covered by industry standards.

Third parties may be denied data access based on risk management concerns or other permissible grounds. The CFPB expects that third parties that comply with the data security requirements of the proposed rule or the GLBA Safeguards Framework would not be denied access to data providers' interfaces, and so very few third parties would incur costs related to this provision of the proposed rule.

Restrictions on Use and Retention

Under the proposed rule, third parties would be required to limit their collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. These limitations could reduce some existing uses of both identifiable and deidentified consumer data by third parties, including the sale of covered data and targeted advertising using covered data. The proposed deletion requirements would also reduce the value of data available for product improvement. Several third party small entity representatives highlighted how consumer data can enable the development of new products and services and can inform research and public policy, even when only deidentified data are used for these secondary purposes. Furthermore, firms in the Aggregator Collection reported using consumer data for functions other

[203] 86 FR 56356, 56556 (Oct. 8, 2021).

[204] SBREFA Panel Report at 12.

than transmitting data to data recipients, including the improvement of existing products, the development of new products, and risk management assessments. The proposed rule may limit third parties' use of consumer-authorized covered data for some of these purposes, though third parties can continue to use data that they generated in providing their products and services for these purposes.

The reduction in available data 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—would lose that source of revenue. Though the CFPB does not have data on the number of third parties that share covered data or the amount of revenue generated by sharing consumer data, 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 of the developers that sold data experienced a decline in revenue post-GDPR.[205] Third parties that use covered data for internal marketing of other products and services may also lose a source of revenue. The CFPB does not have data to quantify this impact.

New Financial Data Processing Products or Services Definition

The CFPB's preliminary view is that the activities covered by the proposed 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.[206] Relative to the baseline, the new 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 requests 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.

2. Costs to Consumers

The proposed 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 proposed 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 proposed rule would also require consumers to reauthorize access to their financial data annually, which involves relatively minor costs. In addition, consumers may incur 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.

Changes in Industry Structure

Data providers would face additional compliance costs as a result of the proposed 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.[207]

The proposed rule would exempt depository data providers that have not established a consumer interface. While it is possible that some institutions may choose to cease operations of or decide against establishing a consumer interface rather than bringing their interfaces into compliance with the proposed rule, the CFPB expects that this would be very rare. Ceasing to operate an existing interface for consumers would likely be highly disruptive to customers or may increase other customer service costs for data providers by more than the potential costs of complying with the proposal. The CFPB does not have the data to determine how many data providers might decide not to operate a consumer interface as a result of the proposal.

Many of the largest depository data providers either already offer developer interfaces that meet many of the requirements of the proposal or are developing such interfaces, and thus their additional costs of complying with the proposed rule would be 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 at least 51 million consumers have connected accounts to third parties through credential-free developer interfaces. This count of 51 million consumers likely understates the true number of consumers who have access to credential-free interfaces 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 a developer interface. Second, it does not include consumers at other institutions—not included in the Provider Collection—that have established developer interfaces 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 would 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 proposed rule because the institutions where they have accounts will face limited costs.

[205] 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.*

[206] 15 U.S.C. 45.

[207] To the extent that the costs incurred by data providers and third parties as a result of the proposal are fixed costs, the CFPB expects that those costs would not be passed on to consumers in the form of higher prices. The CFPB does not have information to estimate what proportion of these costs will be fixed or variable; for example, while some providers may incur a fixed cost of building an interface themselves, others may pay a service provider for use of an interface on a per-account basis.

Effects of Greater Information Sharing

If finalized, the proposed rule would enhance third party access to consumers' financial data, which could 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 would likely benefit, but other consumers may be worse off. While the CFPB understands that the use of cash-flow data for underwriting to identify consumers who are a higher risk than traditional credit scores would predict is not common, 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 to some consumers being offered cheaper credit, if, for example, the information accessed from data providers is viewed by third parties 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 information reveals what a lender views as a signal that a consumer is a higher credit risk than it would have assessed without the consumer-authorized information.[208] Even though it would be the consumer's choice whether to authorize access to their covered data, it is possible that a creditor would 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.[209]

Overall, the availability of consumer-authorized data would allow lenders to underwrite and price more efficiently. This would 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 proposed rule, a third party would need to limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization. To collect covered data beyond the one-year period, the third party would 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 would incur a small time cost to reauthorize the collection of their data. As discussed in the *Costs to third parties* section, 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 sharing of their covered data to a third party or that, given the quickly evolving market of third party products and services, consumers decide to use a different app.

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 proposal 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 sharing data that consumers provide to them with other third parties or, more commonly, sharing 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* section, 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.[210] To the extent that the proposal 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.

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 third parties would reduce their use of screen scraping under the proposed rule. This is likely to benefit covered 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 proposed rule is also likely to decrease the per-agreement cost of negotiating data access agreements.

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

[208] For example, Jansen *et al.* (2023) 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* (June 15, 2023), *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 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 proposed rule: third parties would have access to more information which would increase total surplus and would 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.

[209] 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(2) J. Fin. Econ. at 449–74 (2023), *https://doi.org/10.1016/j.jfineco.2022.12.003.* Similarly, Babina, Buchak and Gornall (2023) develop a model showing that when open banking policies enable the addition of banking data to screening or pricing decisions, higher-cost consumers are 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 (May 12, 2023), *https://dx.doi.org/10.2139/ssrn.4071214.*

[210] 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.*

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 ATO fraud is the most likely fraud risk that could be exacerbated by credential-based data access methods such as screen scraping.[211] In ATO fraud, the fraudster 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 proposed rule would lower the risk of ATO fraud, providing a benefit to data providers through reductions in direct liability and decreased fraud insurance premiums, although it is unclear how much ATO fraud is attributed to credential-based screen scraping. The CFPB does not have sufficient data to estimate how much the proposed rule would lower ATO fraud risk and requests comment on the potential benefit for data providers. However, even a small reduction in ATO fraud risk would have large benefits for data providers.[212]

Along with the proposed requirements to access only the data fields necessary to provide the specific product or service, the shift from credential-based screen scraping to developer interfaces would 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. As discussed above, 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.

Reduced Per-Agreement Negotiation Costs and More Standardized Terms of Access

The CFPB understands that negotiating access agreements with 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, the CFPB estimates 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.[213] 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 negotiation costs would decrease under the proposed rule because many features of access agreements would be regulated by the proposed rule and not subject to 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 under the proposed rule nearly all data providers will use standardized agreements and the costs of establishing data access will be limited to ensuring third party risk management standards are satisfied and reviewing the agreements. A non-small entity representative third party commenter stated that the negotiation of these elements represents approximately 20 percent of total negotiation time.[214] Based on this, the CFPB estimates that negotiations under the proposal would require roughly 80 staff hours. The required time may decline substantially over time as market participants and other stakeholders develop standards for certifying compliance with third party risk management standards. While some data providers and third parties may choose to negotiate customized access agreements with third parties, they will generally only do so when the perceived benefits exceed the costs described here. Therefore, the CFPB has preliminarily determined that the proposed rule is likely to reduce the cost of negotiating and signing an access agreement by $26,000 on average.[215] Under the baseline, data providers would have continued to negotiate access agreements with third parties and these benefits would not have applied to those agreements. As discussed in the *Costs to data providers* section, the CFPB expects that the proposed rule will cause data providers to negotiate additional agreements relative to baseline. The cost of additional negotiations is analyzed above.

Restrictions on Third Parties' Use and Retention of Data

The proposed rule would 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.[216] The proposed rule would 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 would also be subject to that limitation, which would limit the availability of covered data for marketing and for the development of new products outside the scope of the original authorization. While the CFPB does not have data to quantify the benefits 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.

[211] 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.

[212] For example, based on the Javelin Strategy 2022 Identity Fraud Study, a 3 percent reduction in ATO fraud risks would generate an expected annual benefit of $340 million for data providers. *See* Javelin Strategy, *2022 Identity Fraud Study: The Virtual Battlegroun*d (Mar. 29, 2022), *https://javelinstrategy.com/2022-Identity-fraud-scams-report.*

[213] This estimate was derived from BLS data showing mean hourly wages for compliance officers ($37.01), general and operations managers ($59.07), lawyers ($78.74), and software developers ($63.91), which, assuming an equal division of hours across these occupations, yields an average composite hourly wage of $59.68. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to an $85.26 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

[214] *See https://www.regulations.gov/comment/CFPB-2023-0011-0042* (last visited Oct. 5, 2023).

[215] This estimate is based on estimated total hourly compensation of $85.26 multiplied by the difference between the median expected hours required at baseline, 385 hours, and the expected hours required under the proposed rule, 80 hours.

[216] 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.

Required Data Security Representations by Third Parties

The proposed rule would 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 would 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.

Benefits to Third Parties

Right To Access Data Through Third Parties

Under the proposed rule, data providers that have consumer interfaces are required to provide data to authorized third parties. Third parties would be able to access data from new data providers that had not made data available under the baseline. Further, the proposal's data reliability requirements would 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 proposed 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 would be able to reach more consumers under the proposed rule's requirement that authorized third parties have access to covered data.

Prohibition on Data Access Fees

The proposed 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 would 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 may 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 would fall by 80 percent under the proposed rule, or an average savings of $26,000 per negotiated connection agreement. This would bring about substantial savings for third parties, particularly data aggregators. The reduction in negotiation costs could 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 proposed 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.[217] As discussed below, the CFPB expects that third party revenue would increase from the removal of unreasonable access caps under the proposed rule. The CFPB does not have data to quantify these benefits for third parties.

[217] 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 their checking accounts more often.

Improved Accuracy of Data

The proposed rule would require that data providers have policies and procedures reasonably designed to ensure the accuracy of data transmitted through its interface. In addition, the proposed rule provides clarifying standards 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 proposed rule would reduce such issues. The proposed rule would 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 would be more likely to have up-to-date data than under the baseline.

The transition away from screen scraping may lead to a reduction in the number of data fields that third parties can access, as described in the *Costs to third parties* section. However, it would lead to more consistency in the data fields that are available across all data providers and in data field formatting, and would reduce costs associated with ensuring that consumer data are accurate. One 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 expects that once compliant developer interfaces are established, third parties would not screen scrape covered financial data under the proposed rule which would 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 proposed rule would 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 would 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. As

discussed below, the CFPB expects that this would 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* section, the proposed rule would prevent data providers from charging fees to consumers or third parties for access to covered data, guarantee access to data from all non-exempted covered data providers through compliant developer interfaces that meet reliability standards, eliminate unreasonable access caps, and improve the accuracy of received data. 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 increase profits for existing third parties and lead to increased entry into the market for third party services.[218]

The proposed 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 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.[219] The CFPB expects that some third party lenders would be able to identify and reach more consumers with low repayment risk under the proposed 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 would generally cease screen scraping for covered financial data under the proposed 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 screen scraping and 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 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. The firms in the Aggregator Collection reported nearly 16 billion screen scraping attempts in 2022. Under the proposed 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 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 would fall under the proposed rule because screen scraping is more costly for third parties than accessing data through developer interfaces, and most third parties would transition to only accessing covered financial data through interfaces.

Increased Standardization

The CFPB expects that the cost of accessing customer data would decrease not only through reductions in negotiation costs and costs per data access attempt, but also because the proposal would incentivize the industry to coalesce around uniform standards for data access. The 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 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 in the long right tail of the fee distribution a small number of data recipients pay substantially more fees than average.[220]

The proposed 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 if the proposed rule accelerates technological standard development by non-governmental groups. This would reduce frictions and costs from 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.

[218] 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, Buchak, and Gornall (2022) 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. May 2023), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4071214.*

[219] 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.*

[220] For example, responses in the Aggregator Collection suggested that a smaller number of data recipients may pay annualized fees totaling several million dollars.

4. Benefits to Consumers

The proposed rule would likely increase consumers' ability to access their 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 would make this sharing possible without consumers revealing their credentials to third parties, reducing the potential harms that consumers may experience due to a data breach. Consumers would also have increased control over how third parties use their data, since third parties would no longer have indefinite authorization to use a consumer's data or use it for reasons other than the primary purpose. The proposal would likely have important secondary benefits for consumers as well, for example through 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 proposal would require covered data providers to facilitate consumer instructions to provide consumer-authorized third parties with covered data. As discussed in the *Benefits to Third Parties* section, consumers' initial account connection attempts through authorized third parties experience high failure rates, and the proposal would benefit both consumers and third parties by guaranteeing consumer-authorized third parties the right to access covered data. Under the proposed rule, data providers are required to offer a developer interface with commercially reasonable performance, including a proper response rate of at least 99.5 percent. This would 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 above, the CFPB expects third parties' costs of establishing connections with data providers would decline as a result of the proposal, and this may benefit consumers to the extent that lower costs are passed through to them.

Further, guaranteed access to consumer-authorized data would likely increase investment in third parties that request that data, providing consumers with more options in the marketplace and increasing competition.[221] As evidenced by the estimated 100 million consumers using third party data access discussed in the *Baseline* section, 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.[222] The CFPB expects that an expanded range of third party products and services would increase competition and innovation, offering important secondary benefits to consumers, including improved credit access and lower prices, discussed below.

Credential-Free Access—Increased Privacy, Reduced Data Breach Risks

Under the proposal, data providers would be required to create an interface that can be used to share consumer-authorized 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. 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.[223] Courts have approved large settlements in cases where data breaches affected financial service providers.[224] 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.[225] Under the proposed 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 consumer-authorized 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.

The CFPB expects the provisions may induce some data providers and third parties 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.

Third Party Limitations on Collection, Use, and Retention—Ability To Be Forgotten, Increased Privacy, More Control Over Use of Own Data

The proposal would increase consumers' control over how their

[221] For example, Babina, Buchak and Gornall (2023) find that after other countries implemented open banking policies, venture capital investment in fintech companies increased 50 percent 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. May 12, 2023), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4071214.*

[222] 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.*

[223] 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.

[224] 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.*

[225] 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/.*

covered data are used by third parties. There is strong evidence that consumers value control over how their personal information is used and thus would benefit from the proposal. 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.'' [226] 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.[227] 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 more control over how their personal information is used and thus would benefit substantially from the proposal. 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 *Costs to consumers* section, 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 lower credit risk and charging them lower prices. It is possible that a consumer would 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.[228] It is possible that many consumers will experience increased access to credit or lower prices under the proposal, to the extent that they are less able to share covered data with third parties under the baseline.[229] Even without the proposal, 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.[230]

The use of consumer-authorized data may also benefit consumers through increased availability and quality of payment services. The availability of consumer-authorized data may improve payment services by, for example, making it easier to sign 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.[231] 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 credit cards for merchants, some of which may be passed through as benefits to consumers.

Increased availability of consumer-authorized data may also lower the costs for a consumer switching financial institutions in search of higher deposit rates, lower fees, better 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.[232] 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.[233]

[226] 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/.*

[227] 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/.*

[228] 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.*

[229] For example, using data from a German fintech lender, Nam (2022) 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 (Nov. 30, 2022), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4278803.*

[230] These requests include requests for information relating to existing accounts, like credit card limit increases, as well as the underwriting of new loans.

[231] For example, Balyuk and Williams (2021) 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* (Nov. 2021), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974749.*

[232] 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* (May 2023), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4443273.* Erel, Liebersohn, Yannelis, and Earnest (2023) 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 (May 26, 2023), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4459621.*

[233] 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

Continued

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 from overdraft and insufficient funds (NSF) fees in 2022.[234] This is despite the availability of at least 397 deposit account products with zero overdraft and NSF fees, with options available in every state.[235]

If the proposal improves consumers' ability to switch providers, it would have two benefits. First, those consumers who switch could 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 [236] 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.[237] If, due to the proposal, 1 percent of consumer deposits were shifted from lower earning deposit accounts to those 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 proposal, consumers were able to switch accounts and avoid 1 percent of the overdraft and NSF fees they currently pay, they would pay at least $77 million less in fees per year.[238]

The second potential way consumers could benefit is through improved prices and service even for consumers who do not switch providers, due to the proposal'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.[239] To estimate the scale of potential benefits from the provisions, if the proposal 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 provisions caused banks to lower overdraft and NSF fees by 1 percent on average, consumers would benefit from at least $77 million in reduced fees annually.

In addition to the effects in the deposit market, under the proposal, a consumer's depository institution would no longer have a potential advantage in underwriting a loan based on the consumer's transaction data, which could 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 would likely 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.[240]

New Financial Data Processing Products or Services Definition

The CFPB's preliminary view is that the 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 could benefit consumers by increasing protections against unfair,

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.*

[234] 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/.*

[235] 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 Sept. 12, 2023), and current account standards, *https://bankon.wpenginepowered.com/wp-content/uploads/2022/08/Bank-On-National-Account-Standards-2023-2024.pdf* (last visited Sept. 12, 2023).

[236] 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.*

[237] 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 Dec. 9, 2022).* 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.*

[238] 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 and 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.

[239] 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, 2013), *https://libertystreeteconomics.newyorkfed.org/2023/04/deposit-betas-up-up-and-away.*

[240] 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(3) Rev. of Fin. at 977–96 (May 2023), *https://academic.oup.com/rof/article/27/3/977/6619575.* The evidence on this subject is mixed, however, as Medina (2020) 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(5) Rev. of Fin. Studies at 2580–2607 (Sept. 10, 2020), *https://academic.oup.com/rfs/article/34/5/2580/5903746.*

deceptive, or abusive acts or practices. The CFPB does not have data to quantify these potential benefits. The CFPB requests 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 benefits to consumers could result from the new definition.

5. Alternatives Considered

The CFPB considered the impacts of several alternatives to the proposal. These include alternatives which 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 deidentified data as an exception to the general limitation standard that otherwise limits retention.[241] The CFPB also considered alternatives specific to small entities, such as exemptions or longer compliance timelines, which are discussed in part VII.

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 improved 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 requests comment on whether any secondary uses should be allowed through an opt-in mechanism. The CFPB also requests comment on how potentially harmful secondary uses could be defined and prohibited under this alternative.

The CFPB also considered an exception to the general limitation standard for retention and use of deidentified data. Relative to the proposal, this alternative would generally benefit third parties by allowing the continued retention and use of deidentified consumer data after the general limitation standard would normally require the deletion of identified data. For example, deidentified data could potentially be used for product improvement or 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 deidentified 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. The CFPB requests comment on whether there should be an exception to the general limitation standard for deidentified data, and if so, how deidentification should be defined to limit risks to consumers.

F. Potential Impacts on Depository Institutions and Credit Unions With $10 Billion or Less in Total Assets, as Described in Section 1026

The proposed rule would require most depositories and credit unions with $10 billion or less in total assets (community banks and credit unions) to maintain a consumer interface and establish and maintain 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. These institutions are also less likely to have a consumer interface and thus more likely to be exempt from the proposed rule, relative to larger data providers. Compared to nondepository data providers of all sizes, these institutions likely 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 smaller institutions, 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.'' [242] 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 all credit unions, 99.6 percent of whom have $10 billion or less in total assets, the CFPB estimates that at least 53 percent of credit unions already use a vendor that offers interfaces for third parties. To measure the size of vendors used, the CFPB estimates that 89 percent of credit unions use a vendor with at least 100 credit union clients, and 94 percent of 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 6 percent of credit unions using smaller vendors—and in particular the 2 percent of credit unions that did not report using a vendor or reported using a vendor with only a single or handful of clients—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 would face comparable costs to establish a developer interface.

The CFPB seeks comment on its analysis of the potential impact on depository institutions and credit unions with $10 billion or less in total assets.

G. Potential Impacts on Consumers in Rural Areas, as Described in Section 1026

To the extent that the compliance costs of the provisions lead to higher fees or reductions in services offered by small banks and credit unions, consumers in rural areas may be disproportionately affected by the proposed rule because 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.[243]

[241] 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.1.

[242] A ''share'' denotes a deposit account held by a credit union, and thus will include the Regulation E covered accounts under the proposal.

[243] Bd. of Governors of the Fed. Rsrv. Sys., *Trends in Urban and Rural Community Banks* (Oct. 4,

Continued

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.[244] It is possible that rural consumers are more likely to have deposit accounts at institutions without online banking platforms. Since these institutions would be exempt from the requirements for data providers in the proposal, rural consumers at these institutions could experience less of both the costs and the benefits of the proposal. Some of the difference in online banking use may also 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.[245] Given that rural 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.[246]

The CFPB seeks comment on its analysis of potential impacts on consumers in rural areas.

VII. Regulatory Flexibility Act Analysis

The Regulatory Flexibility Act (RFA) [247] 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.'' [248] 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.[249] 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.[250] The CFPB has not certified 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 this proposed rule is discussed in part VII.A. The CFPB is also publishing an IRFA. Among other things, the IRFA estimates the number of small entities that will be subject to the proposed rule and describes the impact of that rule on those entities. The IRFA for this proposed rule is set forth in part VII.B.

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 this proposed rule are described in part II.B.

B. Initial Regulatory Flexibility Analysis

1. Description of the Reasons Why Agency Action Is Being Considered

In section 1033 of the CFPA, Congress directed the CFPB to adopt regulations governing consumers' data access rights. The CFPB is issuing this proposed rule primarily to begin implementing the CFPA section 1033 mandate, although the CFPB is also relying on other CFPA authorities for specific aspects of the proposed rule. See part VI.A for additional discussion.

2. Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule

As discussed in part VI.A, the primary purpose of this proposed rule is to implement section 1033 of the CFPA. This proposed 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 greater competition, and support the development of beneficial products and services. The CFPB is issuing this proposed rule pursuant to its authority under the CFPA. The specific CFPA provisions relied upon are discussed in part III.

3. Description and, Where Feasible, Provision of an Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

The small entities affected by the proposed rule would be those that meet the definitions of covered data providers, third parties, or data aggregators. Covered data providers include depository institutions and nondepository institutions. In the case of the new financial data processing product or service definition, it would apply to third parties, data aggregators, or others who 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 would only be subject to the proposed rule if they meet the definitions of covered data provider, third party, or data aggregator. Examples of potentially affected small third parties include entities using consumer-authorized information to underwrite loans, offer budgeting or personal financial management services, or facilitate payments.

For the purposes of assessing the impacts of the proposed rule on small entities, ''small entities'' are defined in the RFA to include small businesses, small nonprofit organizations, and small

2018), *https://www.federalreserve.gov/newsevents/speech/quarles20181004a.htm.*

[244] David Benson *et al., How do Rural and Urban Retail Banking Customers Differ?,* FEDS Notes (June 2020), *https://www.federalreserve.gov/econres/notes/feds-notes/how-do-rural-and-urban-retail-banking-customers-differ-20200612.html.*

[245] Fed. Commc'ns Comm'n, *2020 Broadband Deployment Report* (Apr. 24, 2020), *https://docs.fcc.gov/public/attachments/FCC-20-50A1.pdf.*

[246] 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).

[247] 5 U.S.C. 601 *et seq.*

[248] 5 U.S.C. 603(a). For purposes of assessing the impacts of the proposed rule on small entities, ''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).

[249] 5 U.S.C. 605(b).

[250] 5 U.S.C. 609.

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. Within the financial industry, 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. Outside of the financial industry, 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 proposals under consideration have a maximum size of $47 million in receipts, but the threshold is lower for some NAICS categories.[251] Table 1 shows the number of small businesses within NAICS categories that may be subject to the proposed rule based on December 2022 NCUA and FFIEC Call Report data and 2017 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 would be subject to the proposed rule.

TABLE 1—NUMBER OF SMALL BUSINESSES WITHIN NAICS INDUSTRY CODES THAT MAY BE SUBJECT TO THE PROVISIONS UNDER CONSIDERATION

	Number of entities	Percent of entities
A. Small Depository Firms		
Commercial Banking (522110) and Savings Institutions (522120)	4,706	
< $850M (Assets)	3,566	75.8
Credit Unions (522130)	4,861	
< $850M (Assets)	4,365	89.8
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	
< $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	

[251] 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 report. 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.*

TABLE 1—NUMBER OF SMALL BUSINESSES WITHIN NAICS INDUSTRY CODES THAT MAY BE SUBJECT TO THE PROVISIONS UNDER CONSIDERATION—Continued

	Number of entities	Percent of entities
< $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, the CFPB estimates that approximately 13 percent of the small depositories would not be subject to the proposed rule because they did not have a consumer interface as of December 2022, leaving approximately 6,897 small depositories subject to the proposed rule. The CFPB is not able to estimate with precision the number of small nondepository entities that would be subject to the proposed rule, but expects that approximately 100 small nondepository institutions would be covered data providers subject to the proposed 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 Institutions	522110, 522120, 522130, 522210	$850 million in assets	8,506	6,897
Nondepository financial institutions and data providers.	511210, 522291, 522320	Varies, less than $47 million in annual receipts.	120	100
Third parties	511210, 518210, 522220, 522291, 522292, 522320, 522390, 523110, 523120, 523140, 541214, 541511, 561450.	Varies, less than $47 million in annual receipts.	7,000–10,000	6,800–9,500

4. Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Proposed 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

The proposed rule would impose new reporting, recordkeeping, and other compliance requirements on small entities subject to the proposal. These requirements generally differ for small entities in two classes: data providers and third parties. Part VI.E provides a detailed description of the requirements and estimated compliance costs that would be faced by affected small entities under the proposed rule. These requirements would be imposed on an estimated 6,897 depository data providers, 100 nondepository data providers, and between 6,800 and 9,500 third parties, as shown in Table 2. The proposed requirements and their costs are summarized in this section.

Requirements for Data Providers

The proposed rule would require data providers to report the number of proper responses divided by the total number of queries to their developer interface on a monthly basis. The CFPB estimates that data providers may face a $7,300 cost of developing and testing a system to regularly disclose this performance metric on their websites. The CFPB expects these reports will generally be automated and will have minimal ongoing costs after the system is implemented.

The proposed rule would require data providers to have policies and procedures to retain records to demonstrate compliance with certain other requirements of the proposed rule. Data providers would 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 would 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 would cost $5,500 to $11,900 per data provider.

The proposed rule requires data providers to establish and maintain a consumer interface that allows consumers to export their covered data in machine-readable formats. As discussed in part VII.B.4, 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 proposed rule requires data providers to establish and maintain a developer interface. As described in part VII.B.4, the CFPB expects that data providers will either contract with a vendor for their developer interfaces or develop and maintain their developer interfaces in-house. The cost estimate of developing and maintaining a developer interface is up to $24 per account per year for small data providers that choose to contract with a vendor. For small data providers that choose to build their developer interface in-house, the estimated upfront cost is between $250,000 and $500,000. Estimated annual costs for in-house developer interfaces include technology costs of $20,000 as well as ongoing staffing costs of $45,000 to $91,000. The proposed rule would require data providers to report the number of proper responses divided by the total number of queries to their developer interface on a monthly basis. The CFPB estimates that data providers may face a $7,300 cost of developing and testing a system to

regularly disclose this performance metric on their websites, with minimal maintenance costs after the system is implemented.

The proposed rule would require 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 would 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 proposed rule. The CFPB understands that most third parties maintain similar records and costs would be limited to a one-time change to existing systems and small storage costs. The CFPB estimates a one-time cost of $8,200 for third parties to develop and implement appropriate policies and procedures, with minimal ongoing costs.

The proposed rule would require third parties to establish and maintain systems that could 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 would be between $21,900 and $91,300, with minimal ongoing costs.

The proposed rule would require 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 $91,300. 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 $2,700 and $3,700.

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.

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.

5. Identification, to the Extent Practicable, of All Relevant Federal Rules Which May Duplicate, Overlap, or Conflict With the Proposed Rule

The Equal Credit Opportunity Act (ECOA) [252] and the CFPB's implementing regulation, Regulation B (12 CFR part 1002), prohibit creditors from discriminating in any aspect of a credit transaction, including a business-purpose transaction, on the basis of race, color, religion, national origin, sex, marital status, age (if the applicant is old enough to enter into a contract), receipt of income from any public assistance program, or the exercise in good faith of a right under the Consumer Credit Protection Act.[253]

EFTA and the CFPB's implementing regulation, Regulation E, establish a basic framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems. Among other requirements, EFTA and Regulation E prescribe requirements applicable to electronic fund transfers, including disclosures, error resolution, and rules related to unauthorized electronic fund transfers.

The FCRA and the CFPB's implementing regulation, Regulation V (12 CFR part 1022), govern the collection, assembly, and use of consumer report information and provide the framework for the consumer reporting system in the United States. They also promote the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. They also include limitations on the use of certain types of consumer information, limitations on the disclosure of such information to third parties, as well as certain requirements related to accuracy and dispute resolution.

The GLBA and the CFPB's implementing regulation, Regulation P (12 CFR part 1016), require financial institutions subject to the CFPB's jurisdiction to provide their customers with notices concerning their privacy policies and practices, among other things. They also place certain limitations on the disclosure of nonpublic personal information to nonaffiliated third parties, and on the redisclosure and reuse of such information. Other parts of the GLBA, as implemented by regulations and guidelines of certain other Federal agencies (*e.g.,* the FTC's Safeguards Rule and the prudential regulators' Safeguards Guidelines), set 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.

TILA and the CFPB's implementing regulation, Regulation Z, impose requirements on creditors and include special provisions for credit offered by credit card issuers. Among other requirements, TILA and Regulation Z prescribe requirements applicable to credit cards, including disclosures, error resolution, and rules related to unauthorized credit card use.

TISA and the CFPB's implementing regulation, Regulation DD (12 CFR part 1030), apply to depository institutions; TISA and part 707 of the NCUA Rules and Regulations apply to credit unions. Among other things, TISA and Regulation DD prescribe requirements applicable to deposit accounts, including disclosure requirements.

The Real Estate Settlement Procedures Act of 1974 [254] and the CFPB's implementing regulation, Regulation X (12 CFR part 1024), include requirements applicable to mortgage servicers that seek to protect borrowers against certain billing and servicing errors.

6. Description of Any Significant Alternatives to the Proposed Rule Which Accomplish the Stated Objectives of Applicable Statutes and Minimize Any Significant Economic Impact of the Proposed Rule on Small Entities

The CFPB considered several alternatives to the proposed rule that would minimize economic impacts on small entities. These alternatives generally fall into four categories: (1) exemptions from the proposed rule for 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.

For small data providers, the CFPB considered exemptions based on the

[252] 15 U.S.C. 1691 *et seq.*

[253] 15 U.S.C. 1601 *et seq.*

[254] 12 U.S.C. 2601 *et seq.*

number of covered accounts or on total assets. To estimate the potential number of entities and share of accounts that would be exempted under the alternatives, the CFPB uses Call Report data as of the end of December 2022 on the number of FDIC- or NCUA-insured deposit accounts as a proxy for covered accounts at depository data providers. The CFPB expects that depositories make up a large majority of small entity data providers but lacks data to estimate the number and size of small nondepository data providers. The CFPB requests data and evidence on these entities.

Tables 3 and 4 report the share and number of all depositories that would be exempted under the proposed rule and under alternative exemption thresholds, as well as the number and share of small entity depositories—those with less than $850 million in assets—that would be exempted. For the estimates under the proposed rule, banks are estimated to be exempt if they did not report ''Yes'' in response to the question ''Do any of the bank's internet websites have transactional capability, *i.e.,* allow the bank's customers to execute transactions on their accounts through the website?'' in December 2022 FFIEC Call Report data. Credit unions are estimated to be exempt if they did not affirmatively report having ''Online Banking'' or a ''Mobile Application'' or services to offer ''Download Account History'' or ''E-Statements'' electronically in December 2022 NCUA Profile Form 4501A data. These data do not precisely identify which entities may be exempt from the proposal, but the CFPB is not aware of better available data to estimate whether entities are exempt. In addition, because at least some entities not reporting online banking or transactional websites have online banking websites as of the publication of this proposal, this is likely an overestimate of the number of exempt entities. The CFPB requests comment on its estimate of the share of depositories exempted.

TABLE 3—NUMBER OF EXEMPTED ENTITIES UNDER ACCOUNT-BASED ALTERNATIVE EXEMPTION THRESHOLDS CONSIDERED

Exemption threshold	Share of depositories exempted (approx.) (%)	Number of depositories exempted (approx.)	Share of small entity depositories exempted (approx.) (%)	Number of small entity depositories exempted (approx.)	Share of accounts exempted (approx.)[255] (%)
Proposed rule[256]	11	1,061	13	1,033	0.64
Less than 500 accounts[257]	5	479	6	464	0.01
Less than 1,000 accounts	10	964	12	943	0.04
Less than 2,000 accounts	18	1,731	21	1,705	0.15
Less than 3,000 accounts	26	2,492	31	2,460	0.32
Less than 4,000 accounts	32	3,091	38	3,047	0.51
Less than 5,000 accounts	38	3,622	45	3,573	0.72
Less than 10,000 accounts	57	5,407	67	5,302	1.88

TABLE 4—NUMBER OF EXEMPTED ENTITIES UNDER ASSET-BASED ALTERNATIVE EXEMPTION THRESHOLDS CONSIDERED

Exemption threshold	Share of depositories exempted (%)	Number of depositories exempted	Share of small entity depositories exempted (%)	Number of small entity depositories exempted	Share of accounts exempted (approx.)[258] (%)
Proposed rule[259]	11	1,061	13	1,033	0.64
Less than $50 million in assets	27	2,621	33	2,621	0.57
Less than $100 million in assets	40	3,799	48	3,799	1.29
Less than $150 million in assets	48	4,631	58	4,631	1.98
Less than $200 million in assets	55	5,249	66	5,249	2.64
Less than $250 million in assets	60	5,704	72	5,704	3.23

The CFPB has preliminarily determined that the exemption in the proposed rule would best target the exemption to those entities which would face the highest cost of compliance absent the exemption. Small depositories without any digital banking infrastructure would face the highest costs from establishing and maintaining interfaces for both consumer and authorized third party access. While many of these entities would be exempted by alternative account- or asset-based exemptions, the CFPB has preliminarily determined that such alternatives would also exempt some data providers that may be able to comply at lower cost. The CFPB also

[255] This is the number of FDIC- or NCUA-insured deposit accounts that would be exempted divided by the total number of FDIC- or NCUA-insured deposit accounts. Credit cards are not in the numerator or denominator. Commercial deposit accounts are in both the numerator and denominator.

[256] For this analysis, banks are classified as exempt if they do not report ''Yes'' to Item 9 of the Schedule RC–M on their December 2022 Call Report. Credit unions are classified as exempt if they did not report that they have ''Online Banking'' or ''Mobile Application'' for question 2 or ''Download Account History'' or ''E-Statements'' for question 4 under ''Information Technology (IT)'' on their December 2022 NCUA Profile Form 4501A.

[257] The estimates in this table are based on FDIC- or NCUA-insured deposit accounts, as there is no available data on number of covered accounts.

[258] This is the number of FDIC- or NCUA-insured deposit accounts that would be exempted divided by the total number of FDIC- or NCUA-insured deposit accounts. Credit cards are not in the numerator or denominator. Commercial deposit accounts are in both the numerator and denominator.

[259] For this analysis, banks are classified as exempt if they do not report ''Yes'' to Item 9 of the Schedule RC–M on their December 2022 Call Report. Credit unions are classified as exempt if they did not report that they have ''Online Banking'' or ''Mobile Application'' for Item 2 or ''Download Account History'' or ''E-Statements'' for Item 4 under ''Information Technology (IT)'' on their December 2022 NCUA Profile Form 4501A.

expects that the later compliance date for these smaller entities will generally reduce the burden on these entities, mitigating the need for broader exemptions.

Small data providers not excluded from the requirements of proposed part 1033 (because they have a consumer interface) that do not have a developer interface would incur the costs necessary to establish and maintain such an interface. To help offset those costs, the CFPB has considered the alternative of permitting small data providers to charge fees for making covered data available through developer interfaces. The CFPB is proposing, however, to prohibit fees across data providers of all sizes. This is because the CFPB has preliminarily 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 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 whom may be small entities. However, exempting third parties from certain conditions of access under the proposed 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 has 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. Since depositories are defined as small entities if they have less than $850 million in assets, all depository small entities would fall into this compliance date tier by definition. As a result, all depository small entities would have a significant amount of time from the issuance of this proposed rule to come into compliance with the rule. Given the development of credential-free interfaces for third parties by core banking providers and other vendors, the CFPB expects that it will not be overly burdensome for small entity data providers to come into compliance before this date. Alternative compliance dates further into the future would extend the period during which screen scraping and other less secure and less privacy-protective data access methods would continue to be used, creating risks of harm to consumers and data providers.

7. Discussion of Impact on Cost of Credit for Small Entities

The CFPB expects that the proposal may have some limited impact on the cost or availability of credit for small entities but does not expect that the impact would be substantial. The CFPB expects there are several ways the proposal could potentially impact the cost or availability of credit to small entities. First, the provisions 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 market. Second, the proposal could potentially increase the cost of credit for small businesses if the costs of implementing the proposal 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.[260] Small entity representatives did not provide feedback on this topic.[261] The CFPB does not have data to quantify these potential impacts.

The CFPB seeks comment on its analysis of the proposal's impact on the cost of credit for small entities, and requests data or evidence on these potential impacts.

VIII. Paperwork Reduction Act

Under the Paperwork Reduction Act of 1995 (PRA),[262] 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 conducts a preclearance consultation program to provide the general public and Federal agencies with an opportunity to comment on the information collection requirements in 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 proposed rule would create a new 12 CFR part 1033 and amend 12 CFR part 1001. The proposed rule contains seven new information collection requirements.

1. Obligation to make covered data available (proposed § 1033.201), including general requirements (proposed § 1033.301) and requirements applicable to developer interface (proposed § 1033.311).

2. Information about the data provider (proposed § 1033.341).

3. Policies and procedures for data providers (proposed § 1033.351).

4. Third party authorization; general (proposed § 1033.401), including the authorization disclosure (proposed § 1033.411).

5. Third party obligations (proposed § 1033.421).

6. Use of data aggregator (proposed § 1033.431).

7. Policies and procedures for third party record retention (proposed § 1033.441).

The information collection requirements in this proposed rule would be mandatory.

The collections of information contained in this proposed 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

[260] 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,* NBER Working Paper No. 29364 (Nov. 2022), *https://www.nber.org/system/files/working_papers/w29364/w29364.pdf.*

[261] SBREFA Panel Report at 40.

[262] 44 U.S.C. 3501 *et seq.*

www.reginfo.gov. Please submit your comments to OMB at *www.reginfo.gov/public/do/PRAMain* by clicking the link ''Currently under Review—Open for Public Comments'' and using the search function to find the ICR for comment.

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: 17,006.

Estimated Total Annual Burden Hours: 2,040,600 annually and 10,323,120 one-time.

Comments are invited 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. Comments submitted in response to this proposal will be summarized and/or included in the request for OMB approval. All comments will become a matter of public record.

If applicable, the notice of final rule will display the control number assigned by OMB to any information collection requirements proposed herein and adopted in the final rule.

IX. Severability

The CFPB preliminarily 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.

However, this is subject to the following significant exception. The CFPB preliminarily considers data providers' proposed obligations to provide data under 12 CFR part 1033 to authorized third parties to be inseparable from the protections the CFPB is proposing 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 preliminary 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 proposed § 1001.2(b).

List of Subjects

12 CFR Part 1001

Consumer protection, Credit.

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 proposes to amend 12 CFR part 1001 and add 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. Add part 1033 to read as follows:

PART 1033—PERSONAL FINANCIAL DATA RIGHTS

Subpart A—General

Sec.

Subpart B—Obligation to Make Covered Data Available

Subpart C—Data Provider Interfaces; Responding to Requests

Subpart D—Authorized Third Parties

Authority: 12 U.S.C. 5512; 12 U.S.C. 5514; 12 U.S.C. 5532; 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.

§ 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, 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); and

(3) Facilitation of payments from a Regulation E account or Regulation Z credit card.

(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 the consumer obtained from that person.

Example 1 to paragraph (c): A digital wallet provider is a data provider.

(d) *Excluded data providers.* The requirements of this part do not apply to data providers that are depository institutions that do not have a consumer interface.

§ 1033.121 Compliance dates.

A data provider must comply with §§ 1033.201 and 1033.301 beginning on:

(a) [Approximately six months after the date of publication of the final rule in the **Federal Register**], for depository institution data providers that hold at least $500 billion in total assets and nondepository institution data providers that generated at least $10 billion in revenue in the preceding calendar year or are projected to generate at least $10 billion in revenue in the current calendar year.

(b) [Approximately one year after the date of publication of the final rule in the **Federal Register**], for data providers that are:

(1) Depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets; or

(2) Nondepository institutions that generated less than $10 billion in revenue in the preceding calendar year and are projected to generate less than $10 billion in revenue in the current calendar year.

(c) [Approximately two and a half years after the date of publication of the final rule in the **Federal Register**], for depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets.

(d) [Approximately four years after the date of publication of the final rule in the **Federal Register**], for depository institutions that hold less than $850 million in total assets.

§ 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).

Consumer means a natural person. Trusts established for tax or estate planning purposes are considered natural persons for purposes of this definition.

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 an entity 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).

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).

Qualified industry standard means a standard issued by a standard-setting body that is fair, open, and inclusive in accordance with § 1033.141(a).

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 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.

§ 1033.141 Standard setting.

(a) *Fair, open, and inclusive standard-setting body.* A standard-setting body is fair, open, and inclusive and is an issuer of qualified industry standards when it has all of 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 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, 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 some participants may play multiple roles, such as being both a data provider and an authorized third party. The ownership structure of entities is considered in achieving balance.

(3) Due process: 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.

(4) Appeals: An appeals process is available for the impartial handling of appeals.

(5) Consensus: Standards development proceeds by consensus, which is defined as general agreement, but not unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.

(6) Transparency: Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

(7) CFPB recognition: The standard-setting body has been recognized by the CFPB within the last three years as an issuer of qualified industry standards.

(b) *CFPB consideration.* A standard-setting body may request that the CFPB recognize it as an issuer of qualified industry standards. The attributes set forth in paragraphs (a)(1) through (6) of this section will inform the CFPB's consideration of the request.

Subpart B—Obligation to Make Covered Data Available

§ 1033.201 Obligation to make covered data available.

(a) *Obligation to make covered data available.* 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. Compliance with the requirements in §§ 1033.301 and 1033.311 is required in addition to the requirements of this paragraph (a).

(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 debit card 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) if it makes available at least 24 months of such information.

Example 1 to paragraph (a): This category includes amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges.

(b) Account balance.

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

Example 1 to paragraph (c): This category includes a tokenized account and routing number that can be used to initiate an Automated Clearing House transaction. In complying with its obligation under § 1033.201(a), a data provider is permitted to make available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number.

(d) Terms and conditions.

Example 1 to paragraph (d): This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.

(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.

§ 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 benefit of 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 establish and maintain interfaces.* A data provider subject to the requirements of this part must maintain a consumer interface and must establish and maintain 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 specific request.* Upon specific request, a data provider must make available to a consumer or an authorized third party covered data in a machine-readable file that can be retained by the consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party.

Example 1 to paragraph (b): A data provider makes available covered data in a machine-readable file that can be retained if the data can be printed or kept in a separate information system that is in the control of the consumer or authorized third party.

(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 format. The interface is deemed to satisfy this requirement if:

(1) The interface makes available covered data in a format that is set forth in a qualified industry standard; or

(2) In the absence of a qualified industry standard, the interface 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.

(c) *Performance specifications.* The developer interface must satisfy the following performance specifications:

(1) *Commercially reasonable performance.* The performance of the interface must be commercially reasonable.

(i) *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 queries for covered data to the interface must be equal to or greater than 99.5 percent. For purposes of this paragraph (c)(1)(i), all of the following requirements apply:

(A) Any responses by and queries to the interface during scheduled downtime for the interface must be excluded respectively from the numerator and the denominator of the calculation.

(B) 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 adheres to a qualified industry standard.

(C) The total amount of scheduled downtime for the interface in the relevant time period, such as a month, must be reasonable. Indicia that the total amount of scheduled downtime may be reasonable include that the amount adheres to a qualified industry standard.

(D) A proper response is a response, other than any message such as an error message provided during unscheduled downtime of the interface, that meets all of the following 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 that 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 amount of time cannot be commercially reasonable if it is more than 3,500 milliseconds.

(ii) *Indicia of compliance.* Indicia that the performance of the interface is commercially reasonable include that it:

(A) Meets the applicable performance specifications set forth in a qualified industry standard; and

(B) Meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers.

(2) *Access cap prohibition.* 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 and 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 adhere to a qualified industry standard.

(d) *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.

(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) by reasonably denying a consumer or third party access to an interface described in § 1033.301(a) based on risk management concerns. Subject to paragraph (b) of this section, a denial is not unreasonable if it is necessary to comply with section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p–1 or section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801.

(b) *Reasonable denials.* To be reasonable pursuant to paragraph (a) of this section, 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.

(c) *Indicia of reasonable denials.* Indicia that a denial pursuant to paragraph (a) of this section is reasonable include whether access is denied to adhere to a qualified industry standard related to data security or risk management.

(d) *Denials related to lack of information.* A data provider has a reasonable basis for denying access to a third party under paragraph (a) of this section if:

(1) The third party does not present evidence that its data security practices are adequate to safeguard the covered data, provided that the denial of access is not otherwise unreasonable; 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 data security practices.

§ 1033.331 Responding to requests for information.

(a) *Responding to requests—access by consumers.* To comply with the requirement in § 1033.201(a), 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 requirement in § 1033.201(a), 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) Confirm 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).

(c) *Response not required.* Notwithstanding the general rules in paragraphs (a) and (b) of this section, 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 provider has a basis to deny access pursuant to risk management concerns in accordance with § 1033.321(a);

(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).

(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 requirements of this section.

(e) *Mechanism to revoke third party authorization to access covered data.* A data provider does not violate the general obligation in § 1033.201(a) 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. To be reasonable, the revocation method must, at a minimum, 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. Indicia that the data provider's revocation method is reasonable include its conformance to a qualified industry standard. A data provider that receives a revocation request from consumers through a revocation method it makes available must notify the authorized third party of the request.

§ 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. The documentation must:

(1) Be maintained and updated as the developer interface is updated;

(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 specification.* On or before the tenth calendar 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 described in § 1033.311(c)(1)(i) 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 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 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. A data provider is permitted to comply with this 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. 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.

(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 explaining the basis for denial; and

(ii) 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.

(3) *Denials of information requests.* When a data provider denies a request for information pursuant to § 1033.331, the data provider:

(i) Creates a record explaining the basis for the denial; and

(ii) Communicates to the consumer or 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.

(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 qualified industry 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 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 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.

(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 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;

(ii) Records of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable;

(iii) Copies of a third party's authorization to access data on behalf of a consumer; and

(iv) 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.

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) *General requirements.* 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.

(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 that the consumer has requested the third party identified in paragraph (b)(1) of this section 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 § 1033.401(b).

(6) A description of the revocation mechanism described in § 1033.421(h)(1).

(c) *Language access*—(1) *General language requirements.* The authorization disclosure must be in the same language as the communication in which the third party conveys the authorization disclosure to the consumer. Any translation of the authorization disclosure 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 activities.* For purposes of paragraph (a)(1) of this section, the following activities 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 collected 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 qualified industry standard.

(4) *Effect of maximum duration.* If a consumer does not provide the third party with a new authorization as described in paragraph (b)(3) of this section, the third party will:

(i) No longer collect covered data pursuant to the most recent authorization; and

(ii) 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.

(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; and

(3) Servicing or processing the product or service the consumer requested.

(d) *Accuracy.* The 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 qualified industry 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 (g) of this section and the condition in paragraph (h)(3) of this section upon receipt of the notice described in paragraph (h)(2) of this section.

(g) *Ensuring consumers are informed.* (1) The third party will 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 will 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. 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.

(i) Categories of covered data collected;

(ii) Reasons for collecting the covered data;

(iii) Names of parties with which the covered data was shared;

(iv) Reasons for sharing the covered data;

(v) Status of the third party's authorization; and

(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.

(h) *Revocation of third party authorization*—(1) *Provision of revocation mechanism.* The third party will 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. 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.

(3) *Effect of revocation.* Upon receipt of a consumer's revocation request as described in paragraph (h)(1) of this section or notice of a revocation request from a data provider as described in § 1033.331(e), a third party will:

(i) No longer collect covered data pursuant to the most recent authorization; and

(ii) 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(h)(3) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data. Any data aggregator that is retained by the authorized third party after the consumer has completed the authorization procedures must also satisfy this requirement. 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 in a separate communication.

§ 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 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 paragraph (a) of this section, a copy of any data aggregator certification statement provided to the consumer separate from the authorization disclosure pursuant to § 1033.431(c)(2).

Rohit Chopra,

Director, Consumer Financial Protection Bureau.

[FR Doc. 2023–23576 Filed 10–30–23; 8:45 am]

BILLING CODE 4810–AM–P