BILLING CODE: 4810-AM-P

BUREAU OF CONSUMER FINANCIAL PROTECTION

12 CFR Chapter X

[Docket No. CFPB-2020-0034]

RIN 3170-AA78

Consumer Access to Financial Records

AGENCY: Bureau of Consumer Financial Protection.

ACTION: Advance notice of proposed rulemaking.

SUMMARY: Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) provides, among other things, that subject to rules prescribed by the Bureau of Consumer Financial Protection (Bureau), a consumer financial services provider must make available to a consumer information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the provider. The Bureau is issuing this Advance Notice of Proposed Rulemaking (ANPR) to solicit comments and information to assist the Bureau in developing regulations to implement section 1033.

DATES: Comments must be received on or before [**INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

ADDRESSES: You may submit comments, identified by Docket No. CFPB-2020-0034 or RIN 3170-AA78, by any of the following methods:

- *Federal eRulemaking Portal*: *https://www.regulations.gov*. Follow the instructions for submitting comments.
- *Email*: 2020-ANPR-1033@cfpb.gov. Include Docket No. CFPB-2020-0034 or RIN 3170-AA78 in the subject line of the message.

- *Mail/Hand Delivery/Courier*: Comment Intake—Section 1033 ANPR, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552.

Instructions: The Bureau encourages the early submission of comments. All submissions should include the agency name and docket number or Regulatory Information Number (RIN) for this rulemaking. Because paper mail in the Washington, DC area and at the Bureau is subject to delay, and in light of difficulties associated with mail and hand deliveries during the COVID-19 pandemic, commenters are encouraged to submit comments electronically. In general, all comments received will be posted without change to *https://www.regulations.gov*. In addition, once the Bureau's headquarters reopens, comments will be available for public inspection and copying at 1700 G Street NW, Washington, DC 20552, on official business days between the hours of 10 a.m. and 5 p.m. Eastern Time. At that time, you can make an appointment to inspect the documents by telephoning 202-435-9169.

All comments, 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. Comments will not be edited to remove any identifying or contact information.

FOR FURTHER INFORMATION CONTACT: Gary Stein, Office of Consumer Credit, Payments, and Deposits Markets at 202-435-7700; or Will Wade-Gery, Office of Innovation, at officeofinnovation@cfpb.gov or 202-435-7700. If you require this document in an alternative electronic format, please contact *CFPB_Accessibility@cfpb.gov*.

SUPPLEMENTARY INFORMATION:

The Bureau is issuing this ANPR to solicit comments and information to assist the

Bureau in developing regulations to implement section 1033 of the Dodd-Frank Act (section 1033), which provides for consumer access to financial records. The Bureau is issuing this ANPR to solicit stakeholder input on ways that the Bureau might effectively and efficiently implement the financial record access rights described in Section 1033, recognizing that various market participants have helped authorized data access become more secure, effective, and subject to consumer control. While the Bureau expects these trends to continue, there are indications that some emerging market practices may not reflect the access rights described in section 1033. The Bureau is also seeking information regarding the possible scope of data that might be made subject to protected access, as well as information that might bear on other terms of access, such as those relating to security, privacy, effective consumer control over access and accessed data, and accountability for data errors and unauthorized access. The Bureau is also interested in comment on whether and how issues of potential regulatory uncertainty with respect to section 1033 and its interaction with other statutes within the Bureau's jurisdiction, such as the Fair Credit Reporting Act, may be impacting this market to the potential detriment of consumers, and seeks information that may help resolve such uncertainty. The Bureau invites comment on all aspects of this ANPR from all interested parties, including consumers, consumer advocacy groups, industry members and trade groups, and other members of the public.

This ANPR proceeds in five sections. Section I summarizes the Dodd-Frank Act's description of consumer rights to access financial records. Section II provides defined terms for the ANPR. Section III provides an overview of data access, with a particular focus on the authorized data access ecosystem, including the players involved, modes of access, competitive incentives and standard-setting, and consumer impacts. Section IV summarizes the Bureau's actions to date relating to consumer-authorized data access. Section V includes a series of

questions about whether and how the Bureau might most effectively provide regulatory guidance in this area.

As discussed in greater detail in section IV, the Bureau has taken several steps with respect to section 1033, including extensive engagement with stakeholders from a range of perspectives. These include a request for information issued in 2016, a Bureau statement of principles in 2017, and most recently, a February 2020 symposium. The valuable information and comments the Bureau has received through its stakeholder engagement efforts informs section III's discussion of the complex issues raised with respect to effective implementation of section 1033 and the section V questions intended to assist Bureau decisions concerning potential rulemaking.

I. Section 1033

Section 1033 is comprised of five subsections. Section 1033(a) provides that, subject to rules prescribed by the Bureau, 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, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.[1] The information is to be made available in an electronic form usable by consumers. Section 1033(b) then outlines certain exceptions from these general access rights. For example, a covered person may not be required to make available to the consumer

[1] Section 1002 of the Dodd-Frank Act defines certain terms used in section 1033. Section 1002(4) defines a "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." 12 U.S.C. 5481(4). Section 1002(5), by incorporation, provides a multi-part definition of "consumer financial products or services." *See* 12 U.S.C. 5481(5). Finally, section 1002(6) defines "covered persons," in part, as entities engaged in offering or providing consumer financial products or services. *See* 12 U.S.C. 5481(6).

"confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors" and "information that the covered person cannot retrieve in the ordinary course of its business with respect to that information."[2]

Section 1033(c) establishes that section 1033 does not "impose any duty on a covered person to maintain or keep any information about a consumer."[3] Section 1033(d) states that "[t]he Bureau, by rule, shall prescribe standards 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."[4] Finally, section 1033(e) requires that the Bureau consult with the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation, and the Federal Trade Commission to ensure, to the extent appropriate, that any rule pursuant to section 1033 imposes substantively similar requirements on covered persons, takes into account conditions under which covered persons do business both in the United States and in other countries, and does not require or promote the use of any particular technology in order to develop systems for compliance.[5]

II. Definitions

This ANPR relies upon several terms defined in the Dodd-Frank Act. For convenience, this ANPR also defines several additional terms. The non-statutorily defined terms in this ANPR

[2] *See* 12 U.S.C. 5533(b)(1) and (4).

[3] 12 U.S.C. 5533(c).

[4] 12 U.S.C. 5533(d).

[5] *See* 12 U.S.C. 5533(e). The Bureau works with other regulators on innovation matters through various means. For example, the Bureau and the OCC recently convened virtual innovation office hours so that participants would have an opportunity to discuss issues that touch upon both consumer protection and prudential regulation. *See* https://www.consumerfinance.gov/about-us/newsroom/cfpb-occ-host-virtual-innovation-office-hours/.

are for purposes of this ANPR only and should not be understood to indicate any legal interpretation, legal guidance, or policy judgment by the Bureau. When specific questions in section V below depart from these definitions, that is specifically noted.

- "Authorized data" means data initially sourced from a data holder as a result of authorized data access.
- "Authorized data access" (or "consumer-authorized data access") means third-party access to consumer financial data pursuant to the relevant consumer's authorization.
- "Authorized entities" are entities or persons with authorized data access to particular consumer financial data.
- "Consumer data access" means authorized data access and direct access.
- "Consumer financial data" (or "consumer data") means "information in the control or possession of [a] covered person concerning a 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."[6]
- "Data aggregator" (or "aggregator") means an entity that supports data users and/or data holders in enabling authorized data access.
- "Data holder" means a covered person with control or possession of consumer financial data.

[6] 12 U.S.C. 5533(a). For purposes of this ANPR, consumer data access involves data that relate to the accessing or authorizing of that consumer's use of a given product or service. As such, references to "consumer data" incorporate the idea of "information in the control of a covered person concerning a consumer financial product or service that [the applicable] consumer has obtained from such covered person."

- "Data user" means a third party that uses consumer-authorized data access to provide either (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer.
- "Direct access" means direct access by the individual consumer to consumer data rather than by an authorized entity.

III. Background

A. Access to consumer financial data

Many providers of consumer financial products and services accumulate information concerning the consumers who use their products and services, the accounts that consumers maintain with them, and other information relating to consumers' use of such products and services. Providers of demand deposit accounts, for example, will accumulate information about the transactions made with a given account and about charges assessed to the account. In many cases, there are well-established statutory and regulatory frameworks that impose requirements on providers of consumer financial products and services to disclose certain information to their customers about their accounts. Disclosure requirements may include, for example, periodic statements with account information on transactions and fees or disclosures about the collection, sharing, use, and protection of consumers' non-public personal information.[7]

[7] *See, e.g.,* Regulation Z, 12 CFR 1026.5(b)(2) and 1026.7(b) (implementing the Truth in Lending Act with respect to periodic statements for credit cards); Regulation E, 12 CFR 1005.9(b) (implementing the Electronic Fund Transfer Act with respect to periodic statements for traditional bank accounts and other consumer asset accounts); Regulation DD, 12 CFR 1030.6(a) (implementing the Truth in Saving Act with respect to periodic statements for deposit accounts held at depository institutions); Regulation P, 12 CFR 1016.4 and 1016.5 (implementing the Gramm-Leach Bliley Act's privacy provisions). Further, on October 5, 2016, the Bureau issued a final rule amending Regulations E and Z for prepaid accounts. For prepaid accounts, the final rule provides an alternative to providing the periodic statement if a financial institution, among other things, makes an electronic history of a consumer's account transactions available to the consumer that covers at least 12 months preceding the date the consumer electronically accesses that account history. The requirement became effective on April 1, 2019.

In addition, consumers wishing to access consumer data[8] can often do so by interacting directly with their consumer financial service providers through providers' online servicing portals or mobile applications. Many providers of consumer financial products and services, from traditional providers like banks and credit unions to newer entrants such as online lenders, make available to consumers extensive electronic data about their use of the institution's products and services. Direct access of this kind is how many consumers now manage their main consumer financial accounts, like their checking accounts, credit card accounts, or mortgage loan accounts.[9]

For some time, a range of companies—including traditional financial institutions and non-bank financial technology, or "fintech," firms—have been accessing consumer data with consumers' authorization and providing services to consumers using data from the consumers' various financial accounts. In recent years, the number and usage of products and services that utilize or rely upon consumers' ability to authorize third-party access to consumer data have grown substantially and rapidly.[10] This growth in authorized data access has been accompanied by expansion in the number of distinct applications or "use cases" for authorized data, including, but not limited to, personal financial management; financial advisory services; assistance in shopping for and selecting new consumer financial products and services; making and receiving

[8] *See supra* note 6.

[9] *See, e.g.*, Lauren Perez, *Online Banking Spikes in Pandemic, With 91% of Americans Banking Virtually in July*, DepositAccounts (Aug. 27, 2020), *available at* https://www.depositaccounts.com/blog/online-banking-spikes-amid-pandemic.html.

[10] *See, e.g.*, The Financial Data and Technology Association of North America, *Competition Issues in Data-Driven Consumer and Small Business Financial Services* (Jun. 2020) at 5-6, *available at* https://fdata.global/north-america/wp-content/uploads/sites/3/2020/06/FDATA-US-Anticompetition-White-Paper-FINAL.pdf.

payments; assisting consumers with improving savings outcomes; identity verification and account ownership validation; credit profile improvement; and underwriting.

This type of consumer-authorized data access and use holds the promise of improved and innovative consumer financial products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services to consumers.[11] Further, stakeholders assert that the increasing ability of consumers to authorize third-party access to consumer data can improve the quality and the consumer experience of consumer financial products and services, expand access and reduce costs related to using those products and services, and further consumer-friendly innovation and competition in consumer financial markets.[12] At the same time, stakeholders have also noted that consumers still face certain potential risks if they authorize access to consumer data, including some risks relating to the methods by which they authorize such access and by which the records are collected and used by authorized entities.[13]

B. Authorized data access ecosystem participants

In authorizing a third party to access consumer data, consumers engage in a broad and complex ecosystem that enables such access. In addition to consumers themselves, the main

[11] *See* Bureau of Consumer Fin. Prot., *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18 2017) (2017 Principles) at 1, *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[12] *See, e.g.*, Bureau of Consumer Fin. Prot., *Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles* (Oct. 18, 2017) (Stakeholder Insights Report) at 4, *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[13] *See, e.g.*, Bureau of Consumer Fin. Prot., *Bureau Symposium: Consumer Access to Financial Records: A summary of the proceedings* (Jul. 2020) (Symposium Summary Report) at 3-7, *available at* https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.

participants in that system are data holders, data users, and data aggregators. A given participant, however, may play more than one—or even all—of these roles.

Data holders include providers of consumer financial products and services that, in the ordinary course of their business, collect, generate, or otherwise possess and retain information about consumers' use of their products and services. In theory, this category could include almost every type of provider of consumer financial products and services. In practice, however, activity in the authorized data access ecosystem to date has focused on banks, credit unions, and other providers of core transaction accounts (especially demand deposit accounts) in their role as data holders.[14] This focus, however, has not been exclusive.

Data users are providers of products and services who use authorized data access to inform or enable the delivery of their products and services. Non-bank fintech companies who offer consumer financial products and services are prominent data users; however, other companies, including banks, also can and do act as data users. As discussed below, data users may use authorized data to enable or seek to improve a wide and growing array of consumer financial products and services, including both those competing in longstanding consumer financial markets as well as innovative products and services in new markets.

Although data users may access consumer data from data holders without the use of any intermediaries, the Bureau understands that currently most authorized data access is effected via data aggregators. These entities access and transmit consumer financial data to data users pursuant to consumer authorization. In some cases, they may also retain consumer data. Data

[14] Consumers may wish to authorize data users to access many more types of data held by many more types of entities. However, the Bureau is concerned in this ANPR only with consumer financial data held by providers of consumer financial products and services.

aggregators are often "fourth parties" that support data users in procuring consumer authorization to access data, and in accessing such data, often support data holders in facilitating authorized third-party access to their customers' data. To date, the market for data aggregation services has primarily focused on aggregators offering services to data user clients[15]; however, as discussed in more detail below, this dynamic has been shifting in recent years towards data aggregators performing services for providers in the providers' capacity as data holders, as well.

Aggregators may play a larger role in the U.S. data access system than in certain other countries because of the relatively large number of bank and credit union data holders in the U.S. and the lack of controlling data standards. Given this multitude of consumer data sources, data users have turned to specialized intermediaries to enable access. In this way, such data users do not have to negotiate access with a large number of data holders with a wide range of data accessibility practices (or in the case of screen scraping, develop and maintain a distinct technical solution for every potential data holder), but instead can contract with one or a handful of aggregators that have already developed and maintain access with respect to many data holders.[16]

---

[15] As recently noted by the OCC, under such arrangements, "[a] data aggregator typically acts at the request of and on behalf of a bank's customer without the bank's involvement in the arrangement." Office of the Comptroller of the Currency, *OCC Bulletin 2020-10: Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29* (Mar. 5, 2020) (OCC Bulletin), *available at* https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html. This has been driven to a significant extent by the primary technical means by which consumer-authorized data access has and continues to be effected; *i.e.*, credential-based access and screen scraping. "Credential-based access" refers to authorized access that uses the consumer's user ID and password or like credentials to log into the data holder's online financial account management portal, generally on an automated basis. "Screen scraping" refers to authorized access that uses proprietary software to convert consumer data presented in the provider's online financial account management portal into standardized machine-readable data, again generally on an automated basis. Credential-based access and screen scraping often are described *collectively* as "screen scraping." But while the two practices typically are linked, they are technically and conceptually distinct.

[16] *See* note 15 (defining "screen scraping").

These three categories—data holder, data user, and data aggregator—are not mutually exclusive in theory or in practice. First, to the extent they collect, generate, or otherwise possess and retain information about their customers in the ordinary course of their business, both data users and data aggregators also may be data holders. For example, a fintech that offers, often on behalf of a depository institution partner, demand deposit accounts to consumers—such fintechs are frequently referred to as "neobanks"—may act as a data user if it obtains, pursuant to consumer authorization, consumer data about a consumer's accounts at other financial institutions to facilitate consumer-directed movement of funds between accounts. But that same neobank may also act as a data holder when one of its consumers authorizes a different financial institution to access consumer financial data at the neobank in connection with applying for a personal loan from that different financial institution. Second, data users may also function as data aggregators, whether they are providing aggregation services purely "in-house" in connection with their own consumer data-supported products and services or if they instead contract with other data users to provide aggregation services.

C. Competitive dynamics and evolving modes of authorized data access

Authorized data access holds the potential to intensify competition and innovation in many, perhaps even most, consumer financial markets. Such intensification can take one of three main forms.

First, authorized data access can enable improvements to existing products. For example, a mortgage lender can improve its products by using authorized data access to verify digitally an applicant's account assets. The consumer is spared the burden of assembling these data and may be able to proceed faster as a result. Additionally, the lender may have greater assurance of data accuracy and reliability.

Second, authorized data access can foster competition for existing products, thereby broadening access, lowering prices, or both. For example, lenders may be able to use consumer data—like deposit account transaction history—to underwrite consumers who might otherwise face more costly credit terms, assuming that they can obtain credit at all. Or a lender might use near real-time account data to provide a consumer with short-term credit options that compete with checking account overdraft functionality and pricing.

Finally, authorized data access can be used to offer new types of products and services. For example, a company may offer an automated personalized financial advice service that consolidates consumer data from across a consumer's various transaction accounts at multiple providers, a service which had only imperfect analogs prior to its development. Of course, many products and services that rely on authorized data access may encompass several or all of the three competitive dynamics.

One notable aspect of the competition fostered by consumer-authorized data access is that in many cases data users may compete for customers with the data holders from which they have obtained data. Sometimes this competition might be direct, as in the example above of a just-in-time lender competing with a bank offering overdraft coverage. Sometimes it might be less direct, as may occur if a bank's customers use a personal financial management application that recommends that some of those consumers shift their business to a competing provider.[17] These competitive dynamics mean that data holders may have an incentive to restrict access by certain data users or to seek greater clarity about the purposes to which particular accessing parties may put accessed data. By the same token, data users may have incentives not to be forthcoming

[17] The intensity of competition may be further affected by the fact that data users may be data holders, as well.

about such purposes.

Of course, these competitive incentives may be outweighed by countervailing incentives. Data holders may have an incentive to provide consumers with the means to enable more secure and controlled authorized data access. Thus, data holders may face consumer demand to allow authorized data access. They also may find that working collaboratively with data users and data aggregators results in a form of authorized data access that is more secure or provides other benefits to data holders.[18] Similarly, data users and aggregators have incentives to develop secure and reliable means of authorized data access, which may necessitate collaboration with data holders. For example, they may find that screen scraping is technically unreliable or challenging to maintain, compared to modes of authentication and access that require collaboration with data holders.

These competitive dynamics appear to be reflected in evolving modes of authorized data access. To date, most consumer-authorized third parties have accessed consumer data through data holders' digital banking portal using digital banking credentials the consumer shared with third parties. Such access generally requires no formal agreement between data holder and data user or data aggregator.[19] More recently, however, the authorized data access ecosystem has seen the emergence of formal, bilateral access agreements between large aggregators and large

[18] Regulatory requirements may also impact incentives. The OCC notes that even when "a bank is not receiving a direct service from a data aggregator and if there is no business arrangement, banks still have risk from sharing customer-permissioned data with a data aggregator. Bank management should perform due diligence to evaluate the business experience and reputation of the data aggregator to gain assurance that the data aggregator maintains controls to safeguard sensitive customer data." OCC Bulletin.

[19] *See* note 15. Such access can involve some degree of collaboration between data holders and third parties which are seeking access. For example, the Bureau understands that many large banks and aggregators engage in "whitelisting." In this practice, the aggregator identifies its traffic to the bank, which allows the bank to permit the aggregator to access consumer data via credential-based access and screen scraping. Also *see, e.g.*, John Pitts, *OCC did its part to secure customer data. Now it's CFPB's turn.* (Mar. 16, 2020), American Banker, *available at* https://www.americanbanker.com/opinion/occ-did-its-part-to-secure-customer-data-now-its-cfpbs-turn.

data holders, which seek generally to move authorized access away from credential-based access and screen scraping towards tokenized access, commonly through application programming interfaces, or "APIs." (When access is tokenized, a third party seeking access uses unique credentials that other parties cannot use; tokenized access is generally considered more secure than access that depends on using the consumer's own credentials.) In addition, a broad range of ecosystem participants have started to come together to develop standards for data sharing through APIs. Networks or consortia of data holders have begun to acquire or partner with data aggregators to offer access solutions to data holders as well as to their traditional data user clients. These moves may herald a broader move towards multilateral standards for data access, much as network standards function in two-sided payment card markets.

It is not clear, however, how these evolving access practices and standards will affect competition or innovation in markets in which participants use authorized data. It is also unclear how effectively they will address other consumer protection risks that may arise with authorized access, including risks relating to the methods by which consumer data is accessed and the purposes for which data users may use authorized data. Panelists at the Bureau's February 2020 "Symposium on Consumer Access to Financial Records and Section 1033 of the Dodd-Frank Act" (Symposium) identified significant progress on some of these issues and uncertainties by participants within the authorized data access ecosystem. However, they also made clear that participants have sometimes struggled to resolve issues in a manner satisfactory to all impacted parties, and according to some participants, in a manner commensurate with the access rights described in section 1033.[20] Participants expressed a range of perspectives on issues relating to,

[20] The Symposium is described further below at Section IV.C. *See also* Symposium Summary Report.

among others, data security, consumer privacy, data minimization,[21] consumer control and transparent use of consumer data, data accuracy, accountability and liability for errors and other problematic transactions, and the mechanisms by which consumer-permissioned parties access records.[22] For example, Symposium panelists discussed whether and how data holders might respect rights described in section 1033 and also refuse access to an authorized third party for security reasons, such as alleged fraud or deficient security practices.[23] Panelists similarly discussed consumer privacy risks arising from existing modes of authorized data access. Panelists proposed and discussed a variety of approaches and actions the Bureau might consider to address these kinds of issues.[24]

D. Other Laws

There are other Federal laws with potential implications for consumer access to financial records pursuant to section 1033, particularly the authorized data access ecosystem.[25] Although Symposium participants did not always agree on whether or how these laws apply in the area of authorized data access, there was general consensus that the Bureau might need to resolve potential stakeholder uncertainty with respect to application of the following laws and their implementing regulations.

[21] The principle of data minimization invokes the general notion that data users only request, and data holders only share, consumer data necessary to perform the service described to and authorized by the consumer. *See* Symposium Summary Report at 6.

[22] *See, e.g.*, Symposium Summary Report at 3-9.

[23] *See id.* at 8.

[24] *See id.* at 4 & 8.

[25] *See id.* at 6-9.

The Gramm–Leach–Bliley Act

The Gramm–Leach–Bliley Act (GLBA) and the Bureau's implementing regulation, Regulation P, require financial institutions 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.

The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) and its implementing regulation, Regulation V, govern the collection, assembly, and use of consumer report information and provide the framework for the credit reporting system in the United States. They also promote the accuracy, fairness, and privacy of information in the files of consumer reporting agencies.

The Electronic Fund Transfer Act

The Electronic Fund Transfer Act (EFTA) and its 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.

IV. Bureau Actions to Date

The Bureau has not promulgated any regulations to implement section 1033. The Bureau has, however, taken several actions in the interest of consumer access to financial records. The Bureau's approach has focused on identifying and promoting consumer interests in, among other areas, access, control, security, and privacy, while allowing the market to develop without direct regulatory intervention.

A. The 2016 RFI

In 2016, the Bureau published in the *Federal Register* a Request for Information Regarding Consumer Access to Financial Information (2016 RFI) on topics including authorized data access.[26] The 2016 RFI described the authorized data access ecosystem as it existed then, as well as certain risks and issues related to that ecosystem.[27] The questions in the 2016 RFI focused on "current market practices" and on "how [commenters] believe market practices may or should change over time."[28] In response, the Bureau received comments from a broad range of stakeholders, including large and small data holders, their trade associations, data aggregators, account data users, individual consumers, and consumer advocates. The Bureau collected further insights, including from stakeholders, through meetings and oral discussions.

B. The Bureau's 2017 Stakeholder Insights Report and Consumer Protection Principles

In October 2017, the Bureau published two documents about consumer-authorized data access. The first document, entitled "Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles" (Stakeholder Insights Report), summarized comments received in response to the 2016 RFI as well as insights gathered in meetings with market stakeholders.[29] The second document, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (2017 Principles), expressed "the Bureau's vision for… a robust, safe, and workable data aggregation market that

[26] *See* 81 FR 83806 (Nov. 22, 2016).

[27] *See* 81 FR 83808-83809 (Nov. 22, 2016).

[28] *See* 81 FR 83810 (Nov. 22, 2016).

[29] *See* Stakeholder Insights Report.

gives consumers protection, usefulness, and value."[30] The 2017 Principles covered nine topics related to consumer-authorized access: access; data scope and usability; control and informed consent; authorizing payments; security; access transparency; accuracy; ability to dispute and resolve unauthorized access; and efficient and effective accountability mechanisms.[31]

C. The Bureau's 2020 Symposium

Following release of the 2017 Principles, the Bureau continued to monitor developments concerning consumer-authorized data access. To that end, the Bureau held the Symposium in February 2020.[32] Panelists at the Symposium represented large and small banks, data aggregators and their trade groups, fintechs, consumer advocates, and other market observers and researchers, and each made a written submission to the Bureau in advance of the Symposium.[33]

As a follow-up to the Symposium, the Bureau published three documents: first, a report summarizing Symposium proceedings[34]; second, a blog post that offered consumers "key information about how data sharing works, what [consumers] should consider before sharing

---

[30] 2017 Principles at 1.

[31] *See* 2017 Principles at 3-5. In publishing the 2017 Principles, the Bureau noted that the 2017 Principles "do not themselves establish binding requirements or obligations relevant to the Bureau's exercise of its rulemaking, supervisory, or enforcement authority." *Id.* at 2. The Bureau further observed "that many consumer protections apply to this market under existing statutes and regulations. These Principles are not intended to alter, interpret, or otherwise provide guidance on—although they may accord with—the scope of those existing protections." *Id*.

[32] *See* Bureau of Consumer Fin. Prot., *CFPB to Host Symposium on February 26* (Feb. 20, 2020), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-hosts-symposium-february-2020/. This document also contains a list of Symposium panelists.

[33] For panelists' written submissions, see Bureau of Consumer Fin. Prot., *CFPB Symposium: Consumer Access to Financial Records*, *available at* https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/. For a recording of the Symposium, see Bureau of Consumer Fin. Prot., *CFPB Symposium: Consumer Access to Financial Records* (Feb. 26, 2020)*, available at* https://www.youtube.com/watch?v=_bQsdQ0462o.

[34] *See* Symposium Summary Report.

[their] data, and some tips on how [consumers] can best protect [their] data and accounts"[35]; and third, an announcement of the Bureau's intention to publish this ANPR.[36]

D. Stakeholder concerns regarding the consumer-authorized data access ecosystem

The Bureau believes that ensuring consumer access to financial records, consistent with other consumer protections, is important to achieving the Bureau's statutory purpose and objectives. Specifically, the Bureau is charged with "ensuring that consumers have access to markets for consumer financial products and services, and that [such markets] are fair, transparent, and competitive."[37] Congress further instructed the Bureau to exercise its authorities so that "markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation."[38] The Bureau believes that the consumer access to financial records provided in section 1033 is an important component of the overall consumer protection framework established by the Dodd-Frank Act.

Through these information gathering opportunities, stakeholders have raised a number of concerns about the current state and direction of the consumer-authorized data access ecosystem. First, some stakeholders contend that not all consumers are able to authorize access to consumer data in a manner commensurate with the access rights described in section 1033. For example, stakeholders report that certain data fields—including, potentially, "costs, charges and usage

[35] Max Bentovim, *What to consider when sharing your financial data* (Jul. 24, 2020), *available at* https://www.consumerfinance.gov/about-us/blog/what-to-consider-when-sharing-your-financial-data/.

[36] Bureau of Consumer Fin. Prot., *CFPB Announces Plan to Issue ANPR on Consumer-Authorized Access to Financial Data* (Jul. 24, 2020), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-anpr-consumer-authorized-access-financial-data/.

[37] 12 U.S.C. 5511(a).

[38] 12 U.S.C. 5511(b)(5).

data"[39]—are sometimes withheld.[40] Similarly, some stakeholders assert that data holders may be defining permitted "use cases" in ways that conflict with the access rights described in section 1033.[41] Although authorized data access ecosystem participants have moved towards data sharing standards that might help to resolve some of these issues, some stakeholders assert that those efforts will not, as a matter of course, fully effectuate the access rights described in section 1033.[42]

Second, stakeholder positions suggest that issues relating to access rights may not be fully resolvable without accompanying resolution of a series of interconnected issues, such as the security of authorized access to consumer data or how consumers should most appropriately exercise control over authorized access.[43] Here, too, informal efforts by ecosystem participants have effected some improvements over time, but some stakeholders have asserted that Bureau regulatory involvement may be required to resolve some of these questions.[44]

Third, stakeholders have raised questions about the application of other consumer financial laws and regulations to consumer-authorized data access.[45] For example, some Symposium panelists asserted that the law is unclear as to: (1) which parties are liable for

---

[39] 12 U.S.C. 5533(a).

[40] *See, e.g.*, Symposium Summary Report at 3.

[41] *See id.* at 6.

[42] *See, e.g.*, Symposium Summary Report at 4, 9; John Pitts, Panelist Written Submission to the Bureau's 2020 Symposium at 3-4, *available at* https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf; Dan Murphy, Panelist Written Submission to the Bureau's 2020 Symposium at 4, *available at* https://files.consumerfinance.gov/f/documents/cfpb_murphy-statement_symposium-consumer-access-financial-records.pdf.

[43] *See id.* at 6-7.

[44] *See, e.g.*, Symposium Summary Report at 3, 5, 8-9.

[45] *See id.* at 7-8.

unauthorized access under the Electronic Fund Transfer Act and Regulation E, as well as under other provisions of law; (2) if and how the Fair Credit and Reporting Act applies to consumer data in the context of authorized data access; and (3) the manner in which the Gramm-Leach-Bliley Act and its implementing regulations regarding privacy and security apply to data aggregators.[46] Some market stakeholders have alleged that uncertainty, ambiguities, or irresolution relating to these kinds of questions may be impeding consumer data access.

V. Topics on Which the Bureau Seeks Comment

In light of the authorized data access ecosystem's evolution since section 1033 was enacted, the Bureau has determined to commence a process that ultimately could lead to regulations that clarify the Bureau's compliance expectations and help to establish market practices to ensure that consumers have access to consumer financial data. The Bureau is issuing this ANPR to solicit comments and information that will assist the Bureau in developing proposed regulations under section 1033.

The Bureau seeks comment from interested parties—including consumers, consumer advocacy groups, industry participants, and other members of the public—on any (or all) of a number of questions relating to potential rulemaking in connection with section 1033.[47] These comments, together with other outreach and analysis, will help the Bureau to determine how it might formulate potential regulatory interventions to better effectuate consumer access to financial records as described in section 1033. Consumers have an interest in being able to secure data access as provided in section 1033 effectively and in a manner that enables ongoing

[46] *See id*. While the Bureau has certain authorities with regard to the Gramm-Leach-Bliley's privacy provisions, the Bureau has no supervisory, enforcement, or rulemaking authority with regard to the Act's data security provision, 15 U.S.C. 6801, or its implementing regulations.

[47] When responding to a question, please note the question number at the top of the response.

and efficient consumer-friendly market innovation. In considering potential interventions, the Bureau will be mindful of avoiding undue or unnecessary burden on industry, particularly in light of self-regulatory standard-setting work that a broad group of market participants has conducted and continues to conduct and other initiatives that may help to foster a safe consumer-authorized data sharing ecosystem.

The Bureau has grouped questions into nine categories: costs and benefits of consumer data access; competitive incentives; standard-setting; access scope; consumer control and privacy; other legal requirements; data security; data accuracy; and other information. For convenience, the questions (and this introduction) continue to use the defined terms from section II above, except when specifically noted.[48] Questions should be understood as directed to practices and outcomes in the United States (except where specifically noted), but commenters may reference non-U.S. information if they believe that is helpful to illuminate or explain the relevance of their comment to potential regulatory action in the U.S. The Bureau requests that, wherever possible, commenters support their responses with information about market practices (both in the U.S. and elsewhere) and/or other empirical data and analysis. The Bureau further encourages commenters to include in their responses any relevant information regarding the potential costs and benefits of consumer data access to consumers and covered persons. Such information may be qualitative, quantitative, or both.

[48] As noted, section II's defined terms are for purposes of this ANPR and should not be understood to imply any legal interpretation, guidance, or policy judgment by the Bureau.

A. Benefits and costs of consumer data access

1. What are the benefits to consumers from authorized data access? What are the benefits to consumers from direct access? What specific regulatory steps by the Bureau would enhance those impacts and how would they do so?

2. How does authorized data access facilitate competition and innovation in the provision of consumer financial services? What are the impacts of direct access on such competition and innovation? What specific regulatory steps by the Bureau would enhance that impact and how would they do so?

3. What costs to consumers flow from authorized data access? What costs result from direct access? What specific regulatory steps by the Bureau would reduce any such impacts and how would they do so?

4. Are there ways in which authorized data access has limited (or may in the future limit) competition and innovation resulting in harms to consumers? Are there ways in which the development of the ecosystem for authorized data access has caused (or may in the future cause) consumer harm? Are there ways in which direct access has had or may have such impacts? What specific regulatory steps by the Bureau would reduce any such impacts and how would they do so?

5. What should the Bureau learn about the costs and benefits of authorized data access from regulatory experience in State jurisdictions or in jurisdictions outside the United States? What should it learn from such sources with respect to direct access? How should this inform the Bureau's consideration of specific regulatory steps that it might take to implement section 1033?

6. How do the costs and benefits to data holders of authorized data access vary across different covered persons, including community banks and credit unions, and how should these

variances inform the Bureau's actions with respect to implementing section 1033? How do the costs and benefits to data holders of direct access vary across different covered persons and how should these variances inform the Bureau's actions with respect to implementing section 1033?

B. Competitive incentives and authorized data access

7. What reasons are there to believe that competitive incentives will facilitate or undermine authorized data access? What responsive actions should the Bureau take and why?

8. To what extent should the Bureau expect the overlap across data holders, data aggregators, and data users to impact competition and innovation favorably or unfavorably? How should the Bureau take account of such overlap in implementing section 1033?

9. Should the Bureau expect access-related agreements between data holders and other participants in the authorized data access ecosystem to impact competition and innovation favorably or unfavorably? How should the Bureau take account of such impacts in implementing section 1033?

10. Should the Bureau expect data access ecosystem participants to develop and adopt multilateral rules applicable to authorized data access? How should the Bureau expect any such rules to impact competition and innovation and how should the Bureau take account of any such impacts in implementing section 1033?

11. Do customers of smaller data holders receive the same benefits from competition and innovation enabled by authorized data access as do customers of larger data holders? If not, why is that the case? How should any variance inform the Bureau's actions with respect to the implementation of section 1033?

12. Do consumers' individual decisions to authorize data access entail significant negative or positive externalities on other consumers, data holders, data aggregators or data users?[49] If so, what are those externalities and what impact do they have on competition, innovation, and the benefits, costs, and risks faced by consumers? How should such externalities inform the Bureau's actions with respect to the implementation of section 1033?

C. Standard-setting

13. To what extent should the Bureau expect broad-based standard-setting work by authorized data access ecosystem participants to enable and facilitate authorized data access? What favorable or unfavorable impacts to competition and innovation should the Bureau anticipate from such work? How should implementation of section 1033 access rights take account of such broad-based standard-setting by system participants?

14. Should the Bureau seek to encourage broad-based standard setting work by authorized data access ecosystem participants? If so, how should it do so?

15. What steps should the Bureau take to prescribe standards applicable to covered persons to promote the development and use of standardized formats for information that can be obtained by means of section 1033 data access rights? What form should such standards take? Should these standards differ depending on whether data is accessed directly by the consumer or through an authorized entity?

16. What steps, if any, should the Bureau take to promote particular mechanisms of authorized data access? If some mechanisms are more beneficial (or as beneficial but at lower

[49] An externality is a direct effect on the well-being of a consumer from the actions of other consumers.

cost to consumers), what are the obstacles to further adoption of such mechanisms, and what steps should the Bureau take to mitigate such obstacles?

D. Access scope

17. The Dodd-Frank Act defines "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual."[50] Who should be considered "an agent, trustee, or representative" of an individual consumer for purposes of implementing section 1033 access rights? Should any exclusions apply? If so, what exclusions and why?

18. Are there types of data holders that should not be subject to the access rights in section 1033? If so, why? Are there any unique issues for any types of data holders that the Bureau should consider in implementing the access rights provided in section 1033, and if so, how should the Bureau account for such issues?

19. How might the Bureau protect against the exposure of confidential commercial information, information that must be kept confidential by law, or information collected for the purpose of preventing fraud or other illegal conduct while at the same time protecting the access rights provided in section 1033? Should the Bureau's approach differ depending on whether data is accessed by authorized third parties or directly?

20. Apart from any restrictions identified in response to the preceding question, are there data elements to which section 1033 access rights should not apply? If so, which elements and for what reasons? Should any restrictions on access to data elements differ depending on whether data is accessed by authorized third parties or directly?

[50] *See* 12 U.S.C. 5481(4).

21. What information should be considered information that cannot be retrieved in the ordinary course of business? How should a Bureau rule seeking to implement the access rights provided in section 1033 account for such information? Should any such accounting differ depending on whether data is accessed by authorized third parties or directly by consumers?

22. Aside from any restrictions identified in response to earlier questions in this section, should any other restrictions on data access be permitted? For example, should a data holder be permitted to restrict authorized access to consumer data created during, or relating to, certain time periods? Should a data holder be permitted to restrict the frequency with which data can be accessed? If such restrictions should be permitted, how and why should they be permitted? Should any of these restrictions differ depending on whether data is accessed by authorized third parties or directly? Should any of these restrictions differ based on the purpose for which data is accessed?

23. Should the Bureau propose to address the operational reliability of authorized data access, and if so, how and why? Should the Bureau consider any different ways to address the operational reliability of direct access, and if so, how and why?

24. How should the Bureau ensure that any implementation of section 1033 access rights does not promote or require the use of particular access (or other) technologies?

E. Consumer control and privacy

With respect to questions in this section, the Bureau encourages commenters to identify, where applicable, the extent to which their responses may differ between primary and secondary uses of authorized data, where primary use reflects the primary purpose for which a consumer, acting pursuant to reasonable expectations, would choose to authorize access to consumer data, and secondary use reflects all other purposes for which authorized data may be used. With

respect to secondary uses of authorized data, the Bureau encourages commenters to consider and explain whether their responses differ depending on whether the consumer data remain identifiably associated with the authorizing individual as well as if and how such data may be disassociated. The Bureau also encouragers commenters responding to this section to identify, where applicable, the extent to which their responses may differ between uses of authorized data for the purposes of effecting payments on behalf of consumers and other uses.

25. To what extent does direct access to consumer data pursuant to section 1033 raise any privacy concerns that should be considered by the Bureau?

26. In what respects do consumers understand the actual movement, use, storage, and persistence of authorized data? To what extent do such movement, use, storage, and persistence of authorized data align with reasonable consumer expectations or preferences, including privacy expectations or preferences? What should the Bureau do, if anything, to improve consumer understanding or to effect closer alignment between practice and consumer expectations or preferences? Should the Bureau consider placing any restrictions on the movement, use, storage and persistence of authorized data, and if so, what restrictions and why?

27. To what extent are consumer understanding and expectations informed by the disclosed terms and conditions of authorized data access or other disclosures? What should the Bureau do, if anything, to improve consumer understanding of disclosed terms and conditions or to improve alignment between such terms and conditions and consumer expectations and/or preferences? Should the Bureau consider requiring any specific disclosures in connection with authorized access? If so, please describe the form, content, and other features of such disclosures.

28. What tools can market participants provide consumers to align consumer expectations and preferences with the actual movement, use, storage, and persistence of authorized data, and what steps, if any, should the Bureau take to improve the effectiveness of such tools?

29. What steps, if any, should the Bureau take to address authorized entities combining authorized data with data from other sources? What are the costs, benefits, and risks to consumers from such combining, and how are those costs, benefits, and risks disclosed to consumers? Should the Bureau address such disclosure, and if so, how and why?

30. Should the Bureau propose to address any of the following, and if so, how and why: (i) data aggregators providing authorized data to entities other than in connection with the primary purpose or purposes for which the consumer authorized data access; or (ii) data aggregators retaining consumer data other than in connection with the primary purpose or purposes for which the consumer authorized access?

31. Should the Bureau propose to address any of the following, and if so, how and why: (i) data users providing authorized data to entities other than in connection with the primary purpose or purposes for which the consumer authorized data access; or (ii) data users retaining consumer data other than in connection with the primary purpose or purposes for which the consumer authorized data access?

32. How, if at all, should a Bureau rule implementing section 1033 seek to limit authorized access to the minimum amount of consumer data necessary to effect the purpose of authorizing access as reasonably understood by the authorizing consumer? What are the benefits and risks to consumers, to competition, and to innovation in consumer financial services of such steps? What are the benefits and risks to consumers, to competition, and to innovation if such steps are not taken?

F. Legal requirements other than section 1033

Some questions in this section refer to "regulatory uncertainty." As used in this section, that term refers to potential stakeholder uncertainty about provisions of law *other than* section 1033, including potential uncertainty that may arise because of the potential interaction or overlap between these other provisions and section 1033.

33. How, if at all, are data holders subject to laws or regulations (whether Federal, State, or foreign) that may be in tension with any proposed obligation to make consumer data accessible per section 1033? How, if at all, should the Bureau address such potential tension?

34. To the extent not addressed in your response to the preceding question, is regulatory uncertainty impeding consumer data access, undermining competition or innovation in the provision of consumer financial services, or otherwise impacting benefits or contributing to risks that consumers might derive from authorized access? If so, in what ways? Which legal provisions are the source of any such uncertainty, and what steps, if any, should the Bureau take to resolve any such uncertainty to the benefit of consumers?

35. In what ways, if any, is regulatory uncertainty around consumer data access imposing costs on consumers, data holders, data users, or data aggregators? Which legal provisions are the source of any such costs, and what steps, if any, should the Bureau take to address any such uncertainty or to mitigate any such costs?

36. What foreign, Federal, or State laws or regulations impose requirements or grant rights that are substantively similar to section 1033? How should the Bureau take into consideration these substantively similar requirements in implementing section 1033? How should the Bureau take account of the conditions under which covered persons do business in the United States and in other countries?

37. To the extent not already addressed above, what actions, if any, should the Bureau take to modify or clarify existing rules that have (or could have) application to consumer data access? What goals would such modification or clarification serve? What costs would they impose or reduce?

G. Data security

38. How effectively does existing law that bears on data security mitigate data security risks associated with data access and, in particular, authorized data access? What steps, if any, should the Bureau take to improve the effectiveness of existing laws that bear on data security in the context of data access?

39. Do data holders, data users, and data aggregators have adequate market incentives to ensure that consumer data is secure? To what extent have they acted on the basis of any such incentives to this point or should be expected to so act going forward?

40. If the Bureau proposes a rule to protect the access rights described in section 1033, how should that rule take appropriate account of data security concerns?

H. Data accuracy

41. To what extent are consumers harmed, or the benefits to consumers of data access endangered or otherwise restricted, by the risk of inaccurate consumer data being provided to consumers or data users? If such harms or restrictions arise, does their extent vary by the type of use to which data is put? If so, why is that the case?

42. Are there risks that some data holders may not have adequate market incentives or legal requirements to ensure that the consumer data they provide to consumers or authorized third parties is accurate and that they correct inaccuracies when they occur?

43. What risks of data inaccuracy are introduced as a result of the data access ecosystem? Do data users and data aggregators have adequate market incentives or legal requirements to ensure that the consumer data they use is accurate or sufficiently accurate for the purposes to which it is put? If your answer varies by the type of use to which consumer data is put, please explain why that is the case. How can data users and data aggregators act on such incentives, to the extent that they exist? To what extent have they so acted to this point or should be expected to so act going forward?

44. What steps, if any, should the Bureau take to address the accuracy of consumer data that as a result of authorized data access is in the control or possession of data aggregators or data users?

45. How effectively does existing law mitigate the risks that inaccurate consumer data is associated with direct access and authorized data access?

I. Other information

46. Is there any other information that would help inform the Bureau as it considers whether to initiate a rulemaking and how best to implement the consumer data access rights provided by section 1033?

VI. Signing Authority

The Director of the Bureau, having reviewed and approved this document, is delegating the authority to electronically sign this document to Laura Galban, a Bureau Federal Register Liaison, for purposes of publication in the *Federal Register*.

Dated: October 22, 2020.

/s/ Laura Galban

Laura Galban,

Federal Register Liaison, Bureau of Consumer Financial Protection.