

February 4, 2021

Acting Director Dave Uejio
Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Consumer Access to Financial Records (Docket No. CFPB-2020-0034)

Dear Acting Director Uejio:

The American Financial Services Association (AFSA)¹ appreciates the opportunity to comment on the Bureau of Consumer Financial Protection’s (Bureau) advance notice of proposed rulemaking (ANPR) to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) entitled, “Consumer Rights to Access Information.”²

AFSA supports innovation in the financial services industry and the ability of consumers to have access to and control over their financial records. At the same time, it is critical that consumers’ financial data be protected. Our comment letter provides feedback on how the Bureau might navigate the line between providing consumers increased access while ensuring that their sensitive information is protected. For example, the Bureau should grant financial institutions³ broad exemption authority under Section 1033(b). Our letter also discusses the interaction between Section 1033 and other federal, state, and international laws and regulations and how a Section 1033 rulemaking might address that interplay so it will benefit consumers. Specifically, we answer Questions #33 and #36 in the ANPR. In addition, our letter includes a discussion on the Fair Credit Reporting Act (FCRA) implications of a Section 1033 rulemaking and addresses the scope of the Bureau’s rulemaking.

I. Section 1033(b) Exceptions

Section 1033(a) provides that, subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, certain financial data. The Bureau should note that all consumers with internet access now have access to their financial data that is with a financial institution with an online platform. A proposed Section 1033 rulemaking arises because the Consumer Financial Act of 2020 defines “consumer” so very broadly that term includes an “agent, trustee, or representative acting on behalf of an individual.”⁴ Section 1033(b) then outlines certain broad exceptions from these general access rights.

The exceptions under 1033(b) include:

- 1) any confidential commercial information, including an algorithm used to derive credit scores or other risk

¹ Founded in 1916, the American Financial Services Association (AFSA) is the national trade association for the consumer credit industry, protecting access to credit and consumer choice.

² The Bureau’s ANPR follows the agency’s Request for Information in 2016 (RFI 2016), the publication of “Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles” (Stakeholder Insights Report) and “Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation” (2017 Principles) in 2017, and the Bureau’s symposium in 2020, “Consumer Access to Financial Records” (2020 Symposium).

³ By “financial institution” we are referring to institutions such as banks and state-licensed finance companies.

⁴ 12 U.S.C. § 5481(4).

- scores or predictors;
- 2) 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;
 - 3) any information required to be kept confidential by any other provision of law; or
 - 4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.

In the plethora of written material regarding Section 1033, the discussion of 1033(b) is surprisingly limited. We hope this is because the exemptions are clear and transparent and little interpretation is needed. AFSA believes that this subsection is crucial to implementing Section 1033 in a manner that ensures the protection of consumers' data. For years there has been a trend in regulation at the international, national, and state levels to better protect consumers' data. AFSA members have spent incredible amounts of time and money enhancing their data protection systems. It seems contrary for a regulation to reverse that trend and require financial institutions to share consumers' data in a manner that puts that data at greater risk of a breach.

Providing consumer data to third parties, such as aggregators, puts that data and hence financial institutions, at considerable risk. Financial institutions are already at risk of having their customer data hacked and sanctioning the opening of that data to aggregators will necessarily heighten that risk. Financial institutions may not be able to perform adequate risk assessments of unregulated third-party data aggregators and should not be burdened with the extraordinary expense of doing so. Section 1033(b) provides a way for financial institutions to manage that risk because it clearly allows them to refuse to provide third parties with access to customer non-public personal information (NPI).

AFSA strongly supports the Bureau implementing rules that construe Section 1033(b) broadly as the statutory language demands. A broad interpretation of Section 1033(b) will allow financial institutions to better protect their customers' data and still comply with the myriad of federal and state privacy laws. Broad exemption authority under Section 1033(b) will not prevent consumers from accessing their own data because they can always directly access their own data; however, it will limit the access of data aggregators to that data, and, in turn, better protect the data. Consumer cannot have privacy unless their data is secured.

Thus, AFSA recommends the Bureau give financial institutions clear authority to decline to share with data aggregators under Section 1033(b). In addition, we recommend the Bureau address section 1033(b)(3) as it relates to exceptions of "any information required to be kept confidential by any other provision of law." Specifically, "any other provision of law" should be defined so it includes both federal and state laws as well as any developed common law.

Furthermore, we suggest that to establish clear consumer control, consent, and disclosure, the Bureau: (a) allow financial institutions to require that their customers consent to data sharing with a third party annually (an opt-in as opposed to an opt-out); (b) have an easy opt-out of any data sharing at any time; and (c) require the data aggregator to disclose to the consumer what data it is gathering and how it will use that data, so aggregators will not use consumers' data in a manner they never contemplated. AFSA is concerned that, without controls, consumers will not understand how their data is being used and by whom. Allowing for annual consents and opt-outs preserves some level of control for consumers.

II. Interaction between Section 1033 and Federal Law

In Question #33 of the ANPR, the Bureau asks, "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?" There is one main

federal law and two implementing regulations whose data protection and privacy obligations create tension with making consumer data accessible under Section 1033: the Gramm-Leach-Bliley Act, Public Law 106-102, (GLBA), the Privacy Rule, and the Safeguards Rule. That tension is outlined below.

A. Gramm-Leach-Bliley Act

AFSA members, as data holders, are governed by the GLBA with respect to their treatment of consumers' NPI. Among other requirements, the GLBA requires financial institutions to ensure the security and confidentiality of customer records and information and protect against unauthorized access.⁵ The GLBA also restricts the disclosure of NPI by financial institutions to nonaffiliated third parties.⁶

Here, Section 1033 states that “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.” Depending on its scope, much of the NPI held by GLBA institutions could be covered by Section 1033(b) and, thus, not susceptible to a Section 1033 request to access. Therefore, any regulation proposed pursuant to Section 1033 should align with the requirements in the GLBA and ensure for the protection of sensitive personal information.

B. Privacy Rule

The “Privacy Rule” is one of the GLBA’s implementing regulations. The GLBA restricts the disclosure of NPI by financial institutions to nonaffiliated third parties.⁷ However, assuming a financial institution obtains consent or acts at the direction of the consumer, permitting disclosure of NPI pursuant to Section 15 of this implementing regulation,⁸ there should be minimal tension between the Privacy Rule and Section 1033. Furthermore, the GLBA allows disclosure of NPI to comply with “federal, state, or local laws, rules, and other applicable legal requirements.”⁹ However, to alleviate questions of whether a lender has proper consent or sufficient direction from a consumer to share his or her data, the Bureau could consider drafting a Model Consumer Consent Form. This form could be provided to the consumer directly by the financial institution, completed by the consumer and directly shared with the financial institution, authenticated, and relied upon.

In addition, the CFPB and its sister regulatory agencies should use their existing powers to make clear that the GLBA’s consumer protections apply to consumer financial data held by all financial institutions, including non-bank innovators that seek to play a role in this ecosystem.¹⁰

C. Safeguards Rule

Another GLBA implementing regulation to which many AFSA members are subject to is the “Safeguards Rule.” It requires protecting the security and confidentiality of the NPI received from a consumer or customer.¹¹ The objectives of the Safeguards Rule are to: (a) insure the security and confidentiality of customer information; (b) protect against any anticipated threats or hazards to the security or integrity of such information; and (c) protect

⁵ 15 USC § 6801.

⁶ *Id.* § 6802; *see also* 12 CFR Part 1016 (Regulation P).

⁷ *Id.* § 6802; *see also* 12 C.F.R. § 1016.10.

⁸ 12 CFR § 1026.15.

⁹ *Id.*

¹⁰ AFSA echoes the comments of its member company, Capital One, on this issue in its comment letter to the CFPB in response to the Bureau’s Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, submitted on Feb. 18, 2020, pp. 5 – 8, available at: https://files.consumerfinance.gov/f/documents/cfpb_heironimus-statement_symposium-consumer-access-financial-records.pdf.

¹¹ *See* 16 C.F.R. part 314.

against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.¹²

A financial institution implements the Safeguards Rule by developing a written information security program appropriate for the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of the customer information.¹³ An important element of such a security program is oversight of service providers who receive NPI from members in the normal course of business. Specifically, a financial institution must:

- (A) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information¹⁴ at issue; and
- (B) Requiring...service providers by contract to implement and maintain such safeguards.¹⁵

No provision in the current iteration of the Safeguards Rule requires a data aggregator to adhere to information security requirements when receiving consumer NPI from a financial institution. To the extent that the CFPB encourages the use of an API interface or similar technology to allow consumer-permissioned access to customer information maintained by a lender, such use may directly conflict with the objectives of the Safeguards Rule described above. APIs themselves may not always be secure.¹⁶ This potentially subjects financial institutions to liability for merely attempting to comply with Section 1033.

Further, promoting dissemination of information by financial institutions to third parties without some oversight of the third party by the financial institution contradicts one required element of the security program, which is oversight over service providers, as described above. A service provider under the Safeguards Rule means “any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.”¹⁷ Presumably, the party seeking the Section 1033 information at the customer’s request would not be deemed a “service provider” unless there was an existing relationship with a financial institution to provide services directly thereto. Thus, under existing regulations, a financial institution does not have any authority to require a Section 1033 requestor, unless also a service provider, to adhere to certain safeguards in protecting customer information. This leaves a substantial gap in the protection of customer information.

D. Recommendations to Address Conflict Between Section 1033 and GLBA

To address the conflict between the requirement to share data under Section 1033 and the requirement to protect data under the GLBA and its implementing regulations, AFSA recommends the Bureau consider one or more of the following options:

1. Directly supervise data aggregators and ensure compliance with the GLBA. The Bureau should directly supervise data aggregators to ensure that they comply with the GLBA and so customer financial data acquired from financial institutions is as protected as it is by the financial institution from whom it came. The Bureau could supervise and examine data aggregators by either: (a) issuing a “larger participant” rule using its authority under Section 1024(a)(1)(B) of the Dodd-Frank Act, or (b) finding that data aggregators pose risks to consumers under its Section 1024(a)(1)(C) authority. With that authority and resource, the

¹² 16 C.F.R. § 314.3(b).

¹³ 16 C.F.R. § 314.3.

¹⁴ “Customer information” under the Safeguards Rule” is defined as “any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates. Note that “you” means “financial institution.”

¹⁵ 16 C.F.R. § 314.4(d).

¹⁶ See *Insecure APIs a Growing Risk for Organizations*, Dark Reading, <https://tinyurl.com/ybz3k6es> (last accessed 1/3/21).

¹⁷ 16 C.F.R. § 314.2(d).

Bureau can better to supervise data aggregators and to ensure that consumers' financial data receives the same protection it is given by financial institutions.

2. Apply the Safeguards Rule to data aggregators. The Bureau should at least make clear that the GLBA and the Safeguards Rule apply to data aggregators. While we believe there are ways that data aggregators could currently fall within the definition, the Bureau and Federal Trade Commission should consider ways to make that clearer.
3. Ensure consumers' consents are up-to-date. As mentioned in Section I above, to establish clear consumer control and consent, the Bureau should allow financial institutions to require their customers' annually consent to data sharing with a third party at the discretion of the financial institution. The Bureau should also ensure that consumers have an easily exercised opt-out of any data sharing at any time.
4. Require that the data holding financial institution not release information to the requestor unless the requestor can provide evidence that it protects the information at a level of security at levels not less than those required by the GLBA and the Safeguards Rule. While an important safeguard of data, this requirement does raise the question of who will monitor a Section 1033 requestor's security levels since a requestor will not be a service provider of a financial institution. This further highlights that the Bureau should undertake the efforts to promulgate a larger participant rule for data aggregators.
5. Draft a form contract. An additional protection may be for the Bureau to draft a form contract or propose mandatory elements of contracts between Section 1033 requestors and financial institutions. In an effort to only capture entities (and not individual persons) in these contractual relationships, only non-human agents and non-natural representatives (excluding trustees) acting on behalf of consumers should be subject to these contractual rules. For example, we would not want to unintentionally subject the personal representative or spouse of a deceased consumer who requests information from financial institutions to these rules. The contract could provide the following provisions:
 - Indemnification with proof of insurance;
 - Error resolution procedures;
 - Outline limits on sharing information as many be relevant under the GLBA (*see* 12 C.F.R. § 1016.11(c)); and
 - Include information on security requirements for the requestor to adhere to when it receives the data (in an effort to mitigate Safeguards Rule concerns).

Recognizing the potential for a conflict between sharing data under Section 1033 and protecting it in accordance with the GLBA and its implementing regulations must be a key part of the Bureau's rulemaking.

III. Interaction between Section 1033 and Foreign and State Laws

In Question #36 of the ANPR, the Bureau asks, "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?" This section of AFSA's comment answers that question.

Many U.S. and international laws and regulations provide individuals with the right to access their information, similar to what a Section 1033 regulation can provide. On the U.S. state level, perhaps the most significant law is the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, and will be significantly

amended on January 1, 2023, as a result of California Proposition 24 also known as the California Privacy Rights Act (CPRA).

Pursuant to California Civil Code § 1798.185(e), the CCPA does not apply to “personal information collected, processed, sold, or disclosed pursuant to the federal GLBA, and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code).” The definition of “personal information” in the CCPA is much broader than the definition of nonpublic personal information in the GLBA context.¹⁸ While the CCPA’s GLBA exclusion tends to exempt much of the information in the possession of GLBA-regulated entities, instances remain in which the GLBA exemption will not apply and, therefore, be subject to the CCPA’s right to access.¹⁹

As noted, depending on its scope, much of the NPI held by institutions that must comply with the GLBA will be covered by Section 1033 and, thus, susceptible to a Section 1033 request for access. However, to the extent that the information is not covered by the GLBA, then it potentially may be covered by both the CCPA and Section 1033, creating a potential for tension between the two.

Importantly, not all financial institutions have chosen to take advantage of the CCPA’s GLBA exemption. For those lenders, the CCPA’s right to access found in California Civil Code § 1798.115 may create tension with any regulations promulgated under Section 1033. That is particularly true since the CCPA’s implementing regulations strictly forbid businesses from disclosing social security numbers, driver’s license numbers or other government-issued identification numbers, financial account numbers, biometric information and account log-in information in response to a CCPA request to access.²⁰ Presumably, this tension would be resolved through the Supremacy Clause.²¹

However, what should not be lost is that the CCPA’s restriction of its own right of access was done to mitigate the risks of identity theft. Indeed, the types of information that the CCPA regulations forbid businesses from turning over to consumers are taken directly from California’s breach notification statute.²² A similar exemption for “covered persons” subject to Section 1033 should be considered. Further, this issue would not just be restricted to California. Statutes similar to the CCPA are being considered by other state legislatures, and all fifty states have breach notification statutes that require entities to notify individuals if there is a security breach involving their personal information. “Covered persons” should not be exposed to a breach notification obligation through a right to access.

In addition, it is expected that more states will enact CCPA-like legislation in the coming years. The “right to access” is found in almost all of the proposed legislation. For example, this right was part of the Washington Privacy Act legislation that failed in 2020. Washington lawmakers have re-filed the Washington Privacy Act in 2021, and similar legislation has been filed in New York and Minnesota. More states are expected to follow.

Another potential area for tension is between the methodology by which a request for access should be validated. For example, the CCPA contains an extensive set of rules that businesses must follow to validate the identity of the individual making a request.²³ Again, requiring covered persons to verify identities ensures the protection of consumers, which must be respected. This extensive set of rules should be considered by the Bureau to ensure disclosure of information to a third party on behalf of a consumer is proper.

¹⁸ Compare Cal. Civ. Code 1798.140(o) with 12 CFR § 1016.3(p) & (q).

¹⁹ See Marci V. Kowski, David M. Stauss and Tobias Moon, California Updates its Privacy Policy, American Bankers Association Risk and Compliance Magazine, August 12, 2019 (analyzing the CCPA’s GLBA exemption and potential gaps).

²⁰ See 11 CCR § 999.313(c)(4).

²¹ See also Cal. Civil Code § 1798.145(a)(1) (stating that the CCPA will not restrict a business’s ability to comply with federal law).

²² See Cal. Civil Code § 1798.82(h).

²³ 11 CCR § 999.323 to .326.

On the international level, the most notable example is the European Economic Area’s General Data Protection Regulation (GDPR). Among other things, GDPR Article 15 provides data subject with the “right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.” GDPR Article 3 states that GDPR can apply extra-territorially. Further, pursuant to guidance issued by the European Data Protection Board, the fact that an individual is located in another country does not necessarily mean that GDPR does not apply.²⁴ Foreign embassies, NATO and the United Nations all have European Union citizens residing in the United States for extended periods.

Further, GDPR is only one international law. Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) provides for the right to access.²⁵ Canada is in the process of amending PIPEDA to strengthen its provisions. Brazil’s Lei Geral de Proteção de Dados or LGPD, which became effective in September, also provides for the right to access and purports to apply extra-territorially.²⁶ Numerous other countries also provide for the right to access in their federal data privacy legislation.

IV. Fair Credit Reporting Act (FCRA) Implications

As noted by the Bureau, “consumer access to [consumer financial records] allows consumers to manage their financial accounts and can enhance consumers’ control of their financial matters. Consumers may realize these benefits by authorizing third parties to access these data on their behalf and allowing those third parties to deliver new or improved financial products and services.”²⁷ Accordingly, companies or other third parties that consumers authorize to access their digital financial records can aggregate those records to offer new products and services aimed at making it easier or more efficient for consumers to manage their financial lives.

More recently, these data aggregators are connecting lenders to consumer bank account data, for various purposes. For example, aggregation services may allow a lender to verify income and assets and perform cash flow analyses more readily. The data may also be used to determine whether a borrower’s financial situation is strengthening to offer additional products or increase a credit line.

With the increasing use of aggregation services, the Bureau has acknowledged a growing tension with the interaction of Section 1033 and the FCRA which regulates access to and sharing of consumer data. The application of the FCRA to consumer-permissioned access to data is arguably uncertain. In particular, there are questions of whether a data aggregator, depending on its activities, is a consumer reporting agency (CRA).²⁸

A central purpose of a data aggregator is to aggregate and monetize the data they have obtained by selling such data to third parties or using it to their own, personal advantage. While such third parties will surely use the information in various ways, there will be some instances in which the information will arguably be used as a consumer report (given the broad definition of consumer report²⁹). If so, the question will be whether that data

²⁴ See European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019.

²⁵ See, e.g., Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 9 – Individual Access.

²⁶ See David M. Stauss, What U.S. Companies Should Know about LGPD – Brazil’s New Data Protection Law, September 16, 2020.

²⁷ Bureau of Consumer Fin. Prot., CFPB Releases Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (Oct. 22, 2020), available at <https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/>.

²⁸ A CRA is “any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.” 15 U.S.C. § 1681a(f).

²⁹ A “consumer report” is broadly defined and means “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a

aggregator is at least “regularly engag[ing]” “in part” “in the practice of assembling information for the purpose of furnishing consumer reports to third parties.” If yes, a regulator or court could take the position that the data aggregator is a CRA subject to the FCRA.

AFSA cautions against this distinction because, if a data aggregator is classified as a CRA, then the question arises as to whether a financial institution responding to a Section 1033 request becomes subject to furnisher responsibilities under the FCRA. A “[f]urnisher” is an entity that furnishes information relating to consumers to one or more consumer reporting agencies for inclusion in a consumer report.”³⁰ On the other hand, the definition of furnisher excludes “a consumer to whom the furnished information pertains.” Thus, very arguably, because the data aggregator will be purportedly acting in the consumer’s stead, it will fall outside the definition. In all events, if classified as a furnisher, the financial institution will be subject to a whole host of obligations, as well as legal risk, including furnishing only “accurate” information, correcting and updating any inaccurate information, and employing a direct dispute mechanism.³¹

Leading up to its issuance of the ANPR, the Bureau sought industry input on how issues of regulatory uncertainty involving Section 1033 and the FCRA may impact the consumer access marketplace. In the Bureau’s February 26, 2020 symposium on “Consumer Access to Financial Records and Section 1033” (Symposium), participants discussed whether aggregators, by collecting and then sharing third-party data to authorized downstream users, would count, at least in some circumstances, as CRAs subject to the FCRA.³²

One consumer advocate argued in the Symposium that if an aggregator collected and shared third-party data that is used or expected to be used as factor in determining eligibility for credit, that aggregator should be considered a CRA, making the data a “consumer report” subject to the FCRA.³³ Advocates argued that the FCRA is the more appropriate governing law because it has a framework for dealing with legal issues relating to accountability for data errors and unauthorized access, through its dispute and adverse action provisions. Section 1033, on the other hand, does not address these issues, potentially making it more difficult for consumers to maintain proper control over their data if aggregated data is not subject to the FCRA.³⁴ At the same time, we note that consumers have dispute rights for their data under Regulation Z and Regulation E.

AFSA recognizes that the use of API by data aggregators is in its early stages of development. The Bureau should anticipate significant growth in the field and that data aggregators may expand into credit reporting agencies, inadvertently making furnishers of creditors sharing consumer information. Given this and the Bureau’s acknowledgment of the potential tension between aggregators’ activities under Section 1033 and the application of the FCRA, AFSA recommends that the Bureau rulemaking clarify how and to what extent the FCRA applies to consumer-permissioned or authorized data as well as rules that clarify how and to what extent data aggregators should be considered CRAs. Such clarification is critical to ensuring stakeholders in the consumer reporting industry, including CRAs and users of consumer reports, are clear on the regulatory obligations required to

factor in establishing the consumer's eligibility for--(A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title.”

Purposes authorized under Section 1681(b) include, among others: (a) reviewing or collecting an account of the consumer, “account” meaning a deposit account; (b) using the information, as a potential investor or servicer in connection with a valuation of an existing credit obligation; (c) using the information in connection with a business transaction that is initiated by the consumer; or (d) using the information to review an account to determine whether the consumer continues to meet the terms of the account. 15 U.S.C. § 1681b(a)(3).

³⁰ 12 CFR § 1022.41(c).

³¹ See 15 USC § 1681s-2.

³² Bureau of Consumer Fin. Prot., Bureau Symposium: Consumer Access to Financial Records: A summary of the proceedings (July 2020) (Symposium Summary Report), available at https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.

³³ See, Symposium Summary Report at 6.

³⁴ *Id.*

maintain FCRA compliance. Moreover, because the FCRA gives consumers the ability to dispute or otherwise challenge inaccurate data, if data governed by Section 1033 is not also subject to the FCRA, the Bureau should promulgate additional rulemakings clarifying ways data aggregators should allow consumers to challenge data inaccuracies or errors. One possibility is to have creditors identify aggregators that qualify as CRAs identified in adverse action notices.

Clearly, financial institutions have the authority to condition sharing of information with an aggregator with a prohibition on its use. APIs always include terms and conditions. This is particularly important in this instance, not just in relation to the FCRA, but also because financial institutions credit models could be reverse engineered.³⁵

In particular, the Bureau should consider issuing clarifications concerning the following circumstances that aggregators use as arguments for why they are not CRAs:

A. Information conveyed at the consumer's request and not furnished to third parties.

CRAs, among other things, must furnish consumer information to a third party. The FTC previously issued guidance that “an entity acting as an intermediary on behalf of the consumer who has initiated a transaction does not become a CRA when it furnishes information to a prospective creditor to further the consumer’s application” and thus, “a mortgage broker does not become a CRA by furnishing consumer reports to prospective creditors on behalf of a consumer that has sought the broker’s assistance in obtaining a loan.”³⁶

Certain data aggregators take the position that if they provide an aggregation product that allows a consumer to choose “permitted” third parties to receive a consumer’s bank data, the aggregator is simply acting as a conduit when it shares the consumer’s data with the permitted financial institution. However, data aggregators may vary in how they develop user experience flows intended to capture the consumer’s authorization for sharing to permitted third parties, with some going into more detail than others on when the consumer gives the express authorization to share. The Bureau should issue consistent and clarifying rules on how aggregation user experience flows should capture consumer authorization to take the authorized data outside of the FCRA’s scope.

B. Assembling or evaluating information.

Typically, an entity is considered a CRA if it, among other things, “assembles or evaluates” consumer information.³⁷ According to the FTC, “assembling” is defined as “gathering, collecting, or bringing together consumer information such as data obtained from CRAs or other third parties, or items provided by the consumer in an application.”³⁸ And further, “evaluating” is defined as “appraising, assessing, determining, or making a judgment on such information.”³⁹ FTC guidance explains that an “entity that perform only mechanical tasks in connection with transmitting consumer information is not a CRA because it does not assemble or evaluate information.”⁴⁰

Data aggregators may standardize aggregated data to make it easier for lenders to use, including using data classifications; some aggregators take the position that this standardization amounts to a mechanical task and does

³⁵ The ease with which confidential information can be reverse-engineered from algorithmic outputs has increased dramatically, as outlined in Capital One’s response to the ANPR.

³⁶ Federal Trade Commission, 40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations, at 30 (July, 2011), available at <https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf>.

³⁷ *Id.* at 29.

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

not rise to the level of assembling or evaluating. In some instances, however, the standardization may involve making a judgment on how the data aggregator classifies or otherwise presents the data, which could be considered an “evaluation.” Finally, the Bureau should issue consistent and clarifying rules on the circumstances under which standardization by an aggregator does not constitute “assembling” or “evaluating” of consumer information. This risk could be minimized or avoided if a rule under Section 1033 or a larger participant rule for data aggregators prohibits aggregators from engaging in the activities of CRAs.

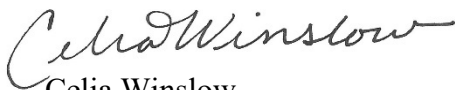
V. Scope of the Bureau’s Rulemaking

AFSA is certain the Bureau recognizes that it requires well more than a modest investment for financial institutions to permit access to the financial records of individuals by their agents, trustees, or representatives. Given the number and varying sizes of the many financial institutions to which the Bureau’s Section 1033 rulemaking will apply, AFSA trusts the Bureau will consider excepting some financial institutions from its applicability.

VI. Conclusion

We appreciate the time and attention that the Bureau has given this rulemaking. Given the complexities of the rule, its interaction with international, national, and state laws, and the implications for NPI, such time and attention is warranted. We encourage the Bureau to allow financial institutions to make broad use of the exemption authority granted by Section 1033(b) and to clearly address the conflict between laws and regulations protecting consumer data and Section 1033’s requirement to share it. Please contact me by phone, 202-776-7300, or email, cwinslow@afsamail.org, with any questions.

Sincerely,



Celia Winslow

Senior Vice President

American Financial Services Association