MBA

MORTGAGE BANKERS ASSOCIATION

February 4, 2021

Comment Intake—Section 1033 ANPR
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

Re: Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records
Docket No. CFPB-2020-0034

Dear Acting Director Uejio,

The Mortgage Bankers Association ("MBA")[1] appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (the "Bureau" or "CFPB") advance notice of proposed rulemaking ("ANPR") on consumer access to financial records. MBA shares the Bureau's view on the importance of the authorized data access ecosystem to the consumer financial services market. While not perfect, the existing consumer authorized data access ecosystem, which has evolved without prescriptive regulations, is largely effective. We believe this experience should guide the Bureau's efforts to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Section 1033"). With respect to the specific standards through which data sharing will occur, we urge the Bureau to support ongoing, stakeholder-led efforts to develop universal API-based data access standards, provided these standards ensure all authorized third parties have equal access to data.

I. Benefits of Consumer Authorized Data Sharing

As the ANPR highlights, broad, permissioned access to consumer financial data plays a crucial role in the modern financial services market. For the housing finance industry, technologies that allow businesses to rapidly access and assess consumer financial information have created substantial consumer benefits. From a process standpoint, streamlined access to

[1] The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, DC, the association works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,200 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, credit unions, thrifts, REITs, Wall Street conduits, life insurance companies, and others in the mortgage lending field. For additional information, visit MBA's website: www.mba.org.

consumer financial data allows for faster and more reliable verification of borrower income and assets for underwriting. Greater automation of the underwriting process has improved the efficiency of the loan production process, reducing costs and making for a more convenient consumer experience.

Along with process improvements, the ability to aggregate consumer financial data provides insights that translate into more accurate risk pricing, which can reduce costs to consumers. Further, this data facilitates the development of innovative algorithmic underwriting models that have the potential to use non-traditional data sources or newly discovered data relationships to increase access to credit for currently underserved borrowers. Finally, by making consumer financial data exportable, these technologies allow existing financial service providers and innovative new business models to serve new markets, which benefits consumers by increasing competition.

Together, these developments have the potential to expand the availability and affordability of mortgage credit. To maximize this potential, MBA encourages the Bureau to implement Section 1033 in a way that:

- fosters competition by creating a level playing field for all authorized data users;
- promotes consumer awareness concerning the way data is accessed and used; and
- supports industry efforts to establish API-based access standards that facilitate consumer-authorized data sharing in a manner that is technology-neutral, secure, and otherwise consistent with the data access rights established by Section 1033.

In conjunction with its Section 1033 rulemaking, the Bureau should also work with stakeholders, including relevant regulators, to clarify the appropriate data privacy and data security standards for data aggregators.

II. Level Playing Field

In its efforts to implement Section 1033, the Bureau should strive to ensure all permissioned third party data users have equal access to the consumer-authorized data sharing ecosystem. Absent a bedrock commitment to open access with consumer authorization, practices may evolve in a way that limits certain entities' ability to engage in consumer-authorized data sharing. For example, market forces may produce a system where an entity's ability to access the data-sharing ecosystem depends on the amount of consumer financial data that entity holds or can afford to pay "a toll" to access. Such a system would have the effect of excluding, or increasing costs on, smaller financial institutions that hold less consumer financial data. This would stifle competition and prevent the benefits of data sharing from reaching all consumers.

By promoting an authorized data access framework that places all participants on equal footing, the Bureau can ensure the benefits of authorized data sharing—*e.g.*, innovative

products, greater convenience, etc.—are available to all consumers and their providers of choice. Further, removing barriers that have the effect of discouraging entities from participating in the consumer-authorized data sharing ecosystem will facilitate greater competition, resulting in greater consumer choice and cost savings. Barriers to entry should be limited, and broadly applicable to ensure appropriate data security and privacy standards are met. We also support the rights of the data providers to protect their proprietary intellectual property that may be derived from the broadly accessible consumer data.

Specifically, the Bureau should make clear that consumer-authorized data access cannot be limited through differential pricing, unduly onerous access controls, or other means which make it more difficult for some market participants to access financial data necessary to achieve their consumer-authorized purposes.

III. Consumer Awareness

One common critique of current consumer-authorized data access practices is that consumers may not fully understand what they are agreeing to when they allow third parties to access their financial information. Consumers are often unaware of what data is collected, whether the third party's access will be one-time or ongoing, or how the data collected will be used. For example, a consumer may, as part of an application for credit, provide their account credentials to allow a third-party data aggregator to collect financial data. Using these credentials, the data aggregator will collect data necessary to analyze the consumer's creditworthiness as of the application date (*e.g.*, account balance, income amounts, and sources, etc.). While this is likely consistent with the consumer's expectations at the time consent was given, other actions by the data aggregator may not be. Specifically, the consumer is unlikely to expect that the data aggregator will access and retain information that is not used as part of the underwriting process, retain the credentials and continue to access the account into the future or use the data collected for purposes other than determining the consumer's creditworthiness.

Absent this awareness, consumers are unable to weigh the costs, benefits, and risks of sharing financial data. This makes it difficult, if not impossible, for many consumers to make an informed decision on whether to authorize access to their financial data. Such a result is contrary to the spirit of Section 1033, which conditions third-party data access on consumer consent. Further, a poorly informed consumer base is more likely to lose confidence in data sharing, which is critical to establishing a sustainable data-sharing ecosystem that benefits all stakeholders.

As a threshold matter, the Bureau can foster greater consumer awareness by supporting consumer education. Specifically, consumers should be taught to be intentional in granting access to their financial data. Along with efforts to educate consumers, the Bureau should

require third parties to disclose to consumers what types of data will be accessed; how that data will be used, stored, and protected; and whether that data will be shared.

These reasonable notification requirements are consistent with the notification requirements imposed on financial institutions under federal law. They are also consistent with the scope of Section 1033, which creates data access rights for third parties who are "agent[s], trustee[s], or representative[s] acting on behalf of an individual[.]"[2] The statute's use of these labels, and the qualification that a third party must be acting on the consumer's behalf, suggest, at minimum, a need for transparency regarding the third parties' use of the consumer's financial data. We encourage the Bureau to collaborate with relevant stakeholders, including financial service providers, data aggregators, fin-techs, and consumer advocates, to identify and develop a means to effectuate these notification requirements.

IV. Industry Efforts to Create Universal API Standards

As the ANPR explains, there are two primary methods of consumer authorized data access: credential-based data access ("screen-scraping") and data access through application programming interfaces ("APIs"). While both methods are effectively used by mortgage lenders and servicers, the consumer-authorized data sharing ecosystem is evolving towards wider adoption of API-based data access. For the reasons outlined below, MBA supports this development and strongly encourages the Bureau to implement Section 1033 in a manner that promotes the adoption of API technologies and supports industry efforts to develop these as universal access standards.

It should be acknowledged that screen-scraping technologies were at the initial forefront of the movement enabling more efficient digital underwriting and have thus provided numerous consumer benefits. Many of the companies that facilitate consumer-authorized data sharing through screen-scraping are conscientious and responsible stewards of the information they are authorized to collect. However, screen-scraping naturally presents heightened data security risks.[3] Unlike API-based data access, which allows third parties to access systems of data holders without requiring consumers to disclose their login credentials, screen-scraping requires consumers to provide their account login information. Though specific practices vary, many third-party data aggregators store these credentials, creating a possible cybersecurity risk.

In addition to the heightened data security risk inherent in the use of login credentials, the breadth of access afforded to third parties through screen-scraping creates additional data security risk. Consumer-permissioned screen-scraping facilitates access to any data displayed

[2] 12 U.S.C. § 5481(4).
[3] Responsible firms acknowledge and attempt to mitigate the risks associated with credential-based data access.

in the online account environment. Thus, along with account balances and recent transaction histories, which are mostly depersonalized, screen-scraping technologies provide access to nonpublic personal information, potentially including data such as credit scores, contact information, and account beneficiaries. These items, which can be used to facilitate identity theft, are not accessible through API-based data access.

By its very nature, consumer-authorized data access through screen-scraping allows third parties to collect data that is not subject to Section 1033. For example, information such as promotional offers made to the consumer could be collected through screen-scraping. Presumably, promotional offers and similar informational items fall outside the scope of Section 1033 given that such information is not "information … concerning the consumer financial product or service that the consumer obtained from such covered person[.]"[4] These data items are not "[account] costs, charges and usage data[,]" the types of consumer financial information contemplated by Section 1033. Data such as promotional offers, financial planning tools, and similar informational items are often the product of proprietary formulas and other intellectual property. In this way, they are similar to "confidential commercial information" and other information specifically excluded from Section 1033.[5] Such indiscriminate access is inconsistent with the limited access rights created by Section 1033.

Unlike the broad access provided through screen-scraping, the ability to access account data through API technologies is intentionally limited to certain, pre-determined data fields. Data mapping and other characteristics of an API—*e.g.*, authentication standards, communication protocols, etc.—are determined through a collaborative process involving the data user and data holder. This helps prevent the transfer of data that is not subject to Section 1033, while also ensuring that the data fields accessible through APIs are those that are necessary to produce or process the transaction sought by the consumer.

While the Bureau should encourage the data access ecosystem's shift toward API-based data access, MBA does not believe that the Bureau should mandate particular technologies, access standards, or authentication requirements. These determinations are best left to market participants, who are better positioned to react to technological change. Moreover, a prescriptive, one-size-fits-all approach may have the unintended consequence of deterring beneficial innovation. Instead, the Bureau should implement Section 1033 in a way that supports industry efforts to develop universal API standards with, as noted above, a requirement that such efforts allow for open access. Should it become necessary, the Bureau can assist these efforts by resolving areas of regulatory uncertainty that may arise.

One particularly promising example of such an initiative is currently being led by the Financial Data Exchange ("FDX"), an industry collective with representation from all relevant

[4] 12 U.S.C. § 5533(a).
[5] 12 U.S.C. § 5533(b)(1).

stakeholders, including financial institutions, data aggregators, consumer advocacy groups, and trade associations. FDX seeks to unify "the financial industry around a common, interoperable and royalty-free standard for the secure access of user permissioned financial data[.]" Specifically, the FDX collective is working to develop standards, and a supporting certification program, addressing issues such as security protocols, authentication, and best practices for user experience and consent guidelines. If successful, the resulting API framework would address many of the concerns affecting the current consumer authorized data access ecosystem.

V. Regulatory Clarity

The Bureau should clarify how the data security and privacy requirements established in the Gramm-Leach-Bliley Act ("GLBA") apply to data aggregators—*i.e.*, "entities that support data users and/or data holders in enabling authorized data access."[6] Data aggregators are subject to the GLBA given that they're "significantly engaged" in "financial activities," and thus qualify as "financial institutions."[7] While data aggregators' data security obligations under the GLBA's Safeguards Rule are clear, there is considerable uncertainty concerning how the GLBA's breach notification and liability provisions apply to circumstances where a data aggregator is compromised leading to a loss of sensitive consumer data. Clarity is also needed concerning the scope of the Fair Credit Reporting Act ("FCRA"). Most significantly, it is unclear whether data aggregators constitute "consumer reporting agencies" for purposes of the FCRA. Greater clarity on the status of data aggregators would shed light on the FCRA responsibilities, if any, for the end-users of such data.[8]

These and other gaps in the data security and privacy framework have the potential to undermine consumer confidence in data sharing. MBA encourages the Bureau to work with stakeholders, including relevant regulators, to make clear how these provisions apply to consumer authorized data sharing transactions involving data aggregators.

---

[6] Bureau of Consumer Financial Protection Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records, pg. 6.

[7] For purposes of the GLBA, "financial activities" include financial data processing, transmission, and storage, which are activities regularly performed by data aggregators. 15 U.S.C. § 6809(c), § 6809(3)(A); 12 C.F.R. § 1016.3(1)(1); 12 C.F.R. § 225.28(b)(14).

[8] Given the common understanding of the word "furnish," which involves an affirmative act of providing something, data holders, which passively allow a consumer to allow a third party access to their financial information, would not constitute data "furnishers" for purposes of the FCRA. 12 C.F.R. § 1022.41(a).

VI. Conclusion

MBA appreciates the opportunity to offer feedback on the Bureau's ANPR on consumer access to financial records. We welcome the opportunity to discuss our recommendations further. Please feel free to direct any questions or comments to me directly (pmills@mba.org) or to Justin Wiseman, Managing Regulatory Counsel (jwiseman@mba.org).

Sincerely,

Pete Mills
Senior Vice President
Residential Policy and Member Engagement
Mortgage Bankers Association