



CENTER FOR CAPITAL MARKETS
COMPETITIVENESS

Julie Stitzel
VICE PRESIDENT

1615 H STREET, NW
WASHINGTON, DC 20062-2000
(202) 463-5339
jstitzel@uschamber.com

February 4, 2021

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

Sent via email: 2020-ANPR-1033@cfpb.gov

Re: Consumer Access to Financial Records [Docket No. CFPB-2020-0034]

To Whom It May Concern:

The U.S. Chamber of Commerce’s (“the Chamber”) Center for Capital Markets Competitiveness (“CCMC”) appreciates the opportunity to submit comments in response to the Consumer Financial Protection Bureau’s (“Bureau”) Advance Notice of Proposed Rulemaking (“ANPR”) regarding Consumer Access to Financial Records and implementation of Section 1033 of the Dodd-Frank Act.¹

The financial services industry has long recognized the importance of maintaining secure consumer access to financial information. Consumer access to financial information allows consumers to manage their own finances more effectively. It likewise makes it easier for consumers to choose the best products for their own needs, which in turn supports the competition and innovation that drives further benefit to consumers. We accordingly understand and support the Bureau’s goals as it works to implement Section 1033.

As reflected in the Bureau’s ANPR, it is critically important that customer data access be safe for consumers. The Bureau is right to note concern that “consumers still face certain potential risk 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.”² Financial institutions and other data holders have been sensitive to these concerns. Likewise, relevant regulatory frameworks require financial service companies to appropriately safeguard customer data, including by taking steps to validate a consumer’s identity when they log on to their account. Indeed, as the Bureau knows from its work in this field, these are not small challenges. The Bureau notes that “the authorized data access ecosystem has seen the emergence of formal, bilateral access agreements between large aggregators and large data holders, which seek generally to move authorized access away from credential-based access and screen scraping towards tokenized access, commonly through

¹ Bureau of Consumer Financial Protection, Advance Notice of Proposed Rulemaking, Consumer Access to Financial Records, 85 Fed. Reg. 71003 (Nov. 6, 2020).

² ANPR, 85 Fed. Reg. at 71005.

application programming interfaces, or ‘APIs.’”³ For example, the members of the Financial Data Exchange (“FDX”), a non-profit group of banks, financial technology (“fintech”) firms, and other financial services businesses, have aligned around a single data-sharing standard that reflects its five core principles of user permissioned data sharing: Control, Access, Transparency, Traceability and Security.

We welcome the Bureau’s acknowledgment of this ongoing work by a broad range of stakeholders to develop and refine solutions that enable secure consumer data access, consistent with applicable regulatory obligations. We ask the Bureau to continue to keep this work front of mind as it proceeds with this rulemaking process. By encouraging further industry collaboration, the Bureau will facilitate continued expansion of consumer data access and the benefits that it offers. Conversely, the Bureau risks undermining these efforts—and the associated consumer benefits—if it pursues a regulatory approach that does not allow businesses to develop collaborative and innovative solutions, is inconsistent or in tension with other regulatory requirements, or creates risks to the security of consumer data.

We accordingly write to emphasize four points:

- The Bureau’s approach should leverage competition in the current market and reflect its rapid evolution.
- Any future regulation should be technologically neutral and principles-based.
- The Bureau should coordinate its approach with other agencies.
- The Bureau should prioritize data security.

Analysis

1. The Bureau’s approach should leverage competition in the current market and reflect its rapid evolution.

The Bureau has an important role to play in articulating clear rules of the road for consumer access to financial data, including with respect to the provision of simple, clear, and consistent disclosures and educational materials. As discussed above, however, the Bureau need not start this work from scratch. Rather, financial industry stakeholders have already undertaken an enormous amount of work to develop effective and secure mechanisms for consumer data access. It accordingly is critical that the Bureau consider existing market dynamics, particularly in areas where broad consensus has been reached on consumer data access related issues. The Bureau should not substitute its own judgment where the marketplace has already developed safe approaches to consumer data access that accomplish the goals underlying Section 1033. Instead, the Bureau should empower financial services businesses to continue to innovate, including through the articulation of flexible standards for data security and other foundational elements of safe and effective consumer data access. Moreover, the Bureau should enable the continued rapid evolution in approaches in the marketplace. The Bureau should be careful not to deter or slow down innovation in this field. It particularly should not impose its preferred approach now in a manner that forecloses future improvements, whether

³ ANPR, 85 Fed. Reg. at 71007.

through a direct prohibition or by creating regulatory risk or other headwinds that disincentivize innovation.

2. Any future regulation should be technologically neutral and principles-based.

Clear rules of the road will help market participants continue to develop and deploy cutting-edge innovations that expand secure and effective consumer data access. Given the rapid evolution of the marketplace, however, along with the technical complexity of solutions in this field, the Bureau should avoid locking in a particular technical approach or being overly prescriptive in a manner that forestalls future innovation. We accordingly urge the Bureau to remain technologically neutral in any future rulemaking. Such an approach would allow innovation to continue to flourish, including to address challenges that emerge in the future and to provide benefits that currently are unanticipated. Such a technologically-neutral approach also would be consistent with regulatory approaches in related areas, including data security, where a regulatory consensus has emerged that companies are best suited to determine the appropriate technological means to meet goals established by regulation.

To that end, we would also urge the Bureau to take a principles-based approach to any future regulation implementing Section 1033. The marketplace continues to develop new approaches to customer data access. Given the dynamic and rapidly evolving nature of this field, it would be a mistake to lock in a specific approach by regulation now. Rather, the Bureau should provide clear guidelines that allow innovation and competition to continue to flourish. Any such rule particularly should draw upon the Bureau's 2017 *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, including by confirming that the Bureau will not second-guess good-faith adoption of policies intended to align with those principles.

3. The Bureau should coordinate its approach with other agencies.

Consumer access to financial data implicates the activities of a broad range of financial institutions, fintech firms, service providers, and other companies. These businesses' handling of customer data is subject to numerous different regulatory frameworks administered by numerous different regulatory agencies. It is critically important that these regulatory frameworks be uniform to the greatest extent possible. A patchwork of different data access and data privacy standards would not benefit consumers. It instead would raise compliance costs, inhibit innovation, and create confusion in the marketplace. Regulatory inconsistency also would impair collaboration among companies that are subject to different regulatory frameworks. In short, the likely outcome of such a patchwork would be for companies to pursue lowest-common-denominator solutions that meet the various requirements—but do not provide maximum benefit for consumers.

In contrast, promoting a level regulatory environment across the diverse industries who handle consumer data would be a critical step towards empowering future innovation. The Bureau accordingly should prioritize regulatory harmonization as a key step towards continued rapid advancements in consumer access to financial data. It should work with all relevant regulatory agencies to achieve this important goal. In doing so, it should be prepared to allow other regulators to take the lead role on particular issues where they have either greater expertise or clear legal authority.

4. The Bureau should prioritize data security.

The financial services industry has long prioritized maintaining the security and privacy of consumers' data. Financial institutions and other businesses in the sector make substantial investments each year in technology and personnel to achieve this goal. As a result, the financial services sector has long been a leader in cybersecurity practices within the private sector, with many other sectors drawing upon the best practices developed by financial companies. In addition, the Bureau and other financial regulators have prioritized data security through rulemaking under the Gramm-Leach-Bliley Act, FFIEC guidance, regulatory enforcement actions, and examination. As a result, data security has been a compliance priority in addition to a business imperative.

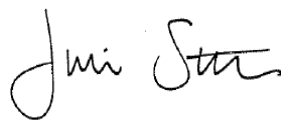
The Bureau should maintain its focus on data security as it proceeds with any rulemaking to implement Section 1033: consumer data access should not come at the cost of the security of the data of the requesting consumer or other customers. In doing so, the Bureau should ensure that uniform and consistent data security standards apply across the various stakeholders in the data sharing ecosystem. As with respect to data access issues more broadly, companies could be subject to a wide range of regulatory regimes. Our members have highlighted requirements established by agencies from the FTC to the FCC, for example, as potentially being implicated.

We would urge the Bureau to clarify which regulatory regimes apply, and when, to the greatest extent possible. In doing so, the Bureau should also focus on promoting the building blocks of data security and privacy in this context, including strong authentication, collection of appropriate consent from users for relevant use cases, and sound mechanisms for demonstrating appropriate authorization. By doing so, the Bureau will help maintain the security of consumer data by allowing companies to follow established security best practices, consistent with applicable regulatory requirements.

* * * * *

We thank you for your consideration of these comments and would be happy to discuss these issues further.

Sincerely,

A handwritten signature in black ink that reads "Julie Stitzel". The signature is written in a cursive, flowing style.

Julie Stitzel