

January 25, 2023

Via Email Submission

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

Re: Comments Regarding Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act – SBREFA Proposals and Outlines

Dear Director Chopra:

The Electronic Transactions Association (ETA) submits these preliminary comments based on the data we currently have in response to the Bureau of Consumer Financial Protection's (CFPB) request for feedback during the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA) panel regarding Section 1033 of the Dodd-Frank Act.

ETA is dedicated to continuously driving innovation in the payment space and values the importance of a financial ecosystem whose participants ensure that consumers and businesses are provided with financial products and services that are convenient, secure, and reliable.

Additionally, ETA members operating globally have already been involved in the creation of open banking frameworks in other jurisdictions, like the UK and Canada, and are determined to share their experiences and challenges, and provide their expertise to help securing the best outcome for US customers and businesses.

ETA appreciates the CFPB's stakeholder engagement and consultation with the industry when detailing the regulatory requirements of the open banking framework and reserves the right to submit comments until a final rule is published. The US is uniquely positioned to learn from the open banking experience and regulatory proposals being adopted or considered by its international counterparts and to adopt best practices and market-led initiatives.

In this regard, ETA commends the CFPB's commitment to investigating the merits of Section 1033 through a process that invites input from the public and other stakeholders and welcomes the opportunity to be part of the dialogue.

Access to financial data and information is an important issue that involves consumers, traditional financial institutions, financial technology companies (fintechs) and other financial service providers, including data aggregators and third-party application providers. And, the ecosystem consists of multiple stakeholders, each with differing roles within data aggregation.

ETA and its members recognize the increased convergence between these groups and the need to preserve consumer access, choice, and control. To preserve market dynamism, ETA strongly encourages the CFPB to be sensitive to the risk of applying a prescriptive regulatory framework and considers the industry is best positioned to lead in addressing these diverse interests. In particular, ETA and its members support an industry-led and principles-based framework for data access that promotes innovation and competition among all industry participants in the financial data marketplace. A data

holder should be modulated based on the amount of data they hold and is protective of consumer interests and safety and soundness. However, as the CFPB works to issue a final rule, ETA urges the CFPB to address and develop a comprehensive liability framework.

Who We Are

ETA is the world's leading advocacy and trade association for the payments industry. Our members span the breadth of significant payments and fintech companies, from the largest incumbent players to the emerging disruptors in the U.S and in more than a dozen countries around the world. ETA members make commerce possible by processing more than \$44 trillion in purchases worldwide and deploying payments innovation to merchants and consumers.

Comments on SBREFA Proposals

Data access scope

While ETA supports industry access to and use of consumer-permissioned data, the critical point is that consumers must have choice and control over how their data is used and shared. The many benefits of innovation should not come at the expense of consumer protection. In this regard, the question of increased access and control over financial data and information must balance important issues such as data security, control, transparency, and disclosure.

Consumers already rely on intermediaries to assist them with data access. And intermediaries are developing additional tools, like consent management dashboards and one-click data deletion, to give consumers even more control over their data. Consumers' choice to use intermediaries to help them manage their financial information should be protected.

Data access must occur in a safe and secure environment. Data recipients must present clear and unambiguous disclosures to the consumer regarding data use, duration of consent, consumer data rights, data security, and all downstream data recipients that will have access to the shared data.

Consumer control, privacy, and liability

With the wider range of market participants accessing consumer financial data, ETA recognizes that the increased choice and improved access to, and enhanced quality of, financial offerings has brought significant benefits to consumers. It may raise concerns, including privacy, cybersecurity, liability, and safety and soundness of the financial sector. Given these potential concerns, ETA and its members believe that the adoption of safe and secure data access methods across the ecosystem and other minimum standards and best practices for the industry will be helpful to alleviate security concerns and corresponding risks, including the risk of fraud in the event of a data breach.

Consumer confidence is directly related to the perception of privacy, security, and protection of financial information and data. Consumers need to be confident in the safety and security of the overall system, and trust that their financial information and data is being used in accordance with their wishes, as long as necessary to provide the service, and that the data and information used is accurate and up-to-date.

ETA recommends the CFPB address and develop a comprehensive liability framework as it works toward publishing a final rule. During this process data aggregators most commonly, have signed data access agreements with banks that transition from credentials-based data access to more secure forms of access



that do not rely on consumer's credentials for data transfer, but may also address issues like liability. Data breach liability is a concern for all participants.

- Is there an allocation of risk between the consumer, data aggregator, and bank that incentivizes all ecosystem participants to protect data? Or is the assumption where the data breach took place is liable?
- Is risk completely overseen by the CFPB or will it be an interagency solution?

The CFPB should adopt and begin to develop a data breach guide. However, any liability guidance adopted by the CFPB should allow market participants the ability to design a process that ensures consumers are made whole in the event of a loss and provides a practical, efficient, and fair means to assign liability, so long as any process or structure does not intentionally or willfully provide any part of the data transfer chain with the authority or influence to impose unfair standards that restrict or inhibit the intent of 1033 and a consumer's request for data portability. Accordingly, the CFPB should align in the principle that liability should follow the data and that all market participants should be collectively liable for the risks they create. We believe that this issue is extremely important and harmonization among consumers complaints needs to be fully addressed.

Data security

Data security is an important consideration that should be addressed in any regulatory framework for data access to consumer-permissioned data. Security and cyber-security risk are increased when financial data is shared with multiple parties and is stored in multiple places, with varying levels of security. Absent an agreement between the parties sharing data, or use of a secure application programming interface (API) or other technology, some service providers rely on other methods to obtain data access information. Current methods of data sharing are not consolidated or principles-based and include, for example, screen scraping as well as API based access. While all of these methods, and their security, may vary from company to company, it is important that they meet industry best practice standards.

Legacy processes, such as credential-based access through screen scraping, are less ideal than credential-less methods of access that enable greater security and clarity over the transmission of data between systems standardized data portals, such as APIs, that allow for more secure transmission of data between systems. As the industry moves towards credential-less access adoption, the CFPB should set principles-based guidelines for industry-led standards to meet. This would permit flexibility over time to accommodate the technology capabilities of various stakeholders and satisfy consumer expectations. Additionally, the CFPB should consider credential-based access as a secondary option in instances where the data is not available via more secure, credential-less methods of access.

Security performance standards need to be developed to ensure technology is sufficient (and continually reviewed), access is limited, consent-based, and storage of data occurs. Similarly, performance of data access portals, for those providers who choose this method of data transfer, needs to be assessed to ensure consumers and authorized third parties receive access that is equal to what the data holder would provide a consumer directly or through its own services. However, it is imperative that technology standards do not mandate a specific type of technology, but remain flexible enough to ensure industry leading safeguards, and allow for innovation.

ETA agrees with the CFPB that nearly all covered data providers already comply with either the FTC Safeguards Rule or Guidelines issued under the Gramm-Leach-Bliley Act, as well as the prohibition

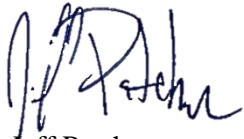


against unfair practices¹. However, the CFPB should establish a framework to set reasonable security standards to address the risk profile of each entity and set a reasonable industry standard approach. It should be done in such a way that allows flexibility to combat future risks and technical flexibility to allow innovation in implementation of the framework. Consumers expect their financial data is subject to protection when held by a financial institution or a non-bank provider of financial services.

* * *

ETA appreciates the opportunity to provide input on this important issue. If you have any questions, please contact me or ETA's Senior Vice President of Government Affairs, Scott Talbott at stalbott@electran.org.

Sincerely,



Jeff Patchen
Director of Government Affairs
Electronic Transactions Association
jpatchen@electran.org
(202) 677-7418

¹ 16 CFR part 314(FTC Safeguards Rule); 12 CFR part 30, App. B (OCC Safeguards Guidelines); 12CFR part 208, App. D-2 (Federal Reserve Board Safeguards Guidelines); 12CFR part 364, App. B (FDIC Safeguards Guidelines); 12 CFR part 748, App. B (NCUA Safeguards Guidelines). The Securities and Exchange Commission and the Commodity Futures Trading Commission also have issued rules implementing GLBA data security standards with respect to the entities under their jurisdiction.