

February 4, 2021

*Via eRulemaking Portal*

Comment Intake – Section 1033 ANPR  
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 – Docket No. CFPB-2020-0034; RIN No. 3170-AA78**

To whom it may concern:

The Electronic Transactions Association (ETA) respectfully submits comments in response to the Bureau of Consumer Financial Protection’s (CFPB) notice of proposed rulemaking in developing regulations to implement 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. 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. As we elaborate further in these comments, ETA considers that 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.

By supporting the consumers’ ability to easily access and share their financial account information it allows them to choose financial products and services that fit their personal financial needs and take more control over their financial lives. The financial applications and services built on consumer-permissioned data are creating greater competition in financial



markets, reducing rates and fees, improving the quality of financial products and services available to consumers, and expanding access to underserved consumers.

## Who We Are

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include banks, mobile payment service providers, mobile wallet providers, money transmitters and non-bank FinTech companies that provide access to credit, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives – facilitating over \$22 trillion in payments in 2019 worldwide.

## Comments on Proposed Rule

### A. Benefits and costs of consumer data access

There are clearly many potential applications and many benefits to be realized by consumers, FinTechs, and financial institutions alike.

First, by being consumer-centric, Section 1033 supports improved efficiency and customer services in the financial services industry by helping parties share data more effectively and increasing not only consumer control over their own information and data but also choice. ETA shares the prevailing view that consumers already benefit from financial innovations that rely on direct access to their personal and financial data.

Secondly, it drives innovation. Over the past several years, ETA members have developed innovative products and services that help consumers manage their financial lives, expand financial offerings and access to financial services, lower costs, improve financial management, provide more affordable options, and increase transaction security. These developments have resulted in a number of benefits for consumers:

- Consumer convenience
- Protecting consumers from fraud
- Empowering consumers to understand and control their financial lives, make useful decisions, monitor spending and debt, and set and achieve savings goals
- Providing consumers with a holistic financial picture of their financial health/product mix
- Helping consumers communicate effectively with their financial service providers
- Helping consumers solve financial problems in timely ways

These benefits extend across a diverse and growing universe of financial products and services, including personal financial management software, online lending platforms, mobile wallets, and fraud and identity theft systems.



More specifically, technological advances have allowed ETA member companies to use consumer account data from multiple accounts held at multiple financial institutions to develop new products and services that empower consumers to manage their finances. At the same time, consumer-permissioned data access allows financial services providers also to see a full financial picture of the consumer and to target the right financial products and services to that consumer. These products and services include:

- Personal financial management tools that allow consumers to use a single account to manage all of their financial accounts
- Savings apps that facilitate automatic savings by consumers
- Budget tools that help consumers set and follow budgets
- Lending services that provide consumers with access to simple loan application and underwriting processes
- Bill payment services that allow consumers to manage all of their bills through a consolidated service
- Investment management services that facilitate investment or education

ETA recommends the CFPB expand direct access to all financial information – with a few guardrails. For example, data minimization and the need for clear and accessible disclosures is paramount in ensuring the integrity of informed consent driven data exchange. Those additional data points create a safer ecosystem for all participants. There are a wide range of use cases beyond information aggregation and payment initiation, including account opening (identity verification and authentication), loyalty integration, account information analytics, as well as tailored marketing solutions that could be implemented when more data sources are used. In many cases, access to consumer and financial institution data is crucial to the success of these new products and services. Having access to consumer data will maximize the usability of products and services but access to additional data creates risks, such as identity theft, fraud, and unauthorized use of consumer account credentials. ETA believes the CFPB should address these concerns before issuing a final rule.

The CFPB is uniquely positioned to learn from the experience and regulatory proposals being adopted or considered by its international counterparts and to adopt best practices and market-led initiatives using examples from those jurisdictions. The CFPB should carefully consider implementing a principle-based framework designed to drive specific market outcomes.

#### B. Competitive incentives and authorized data access

When financial data is shared securely at the direction of consumers, it can help them better manage their finances, while receiving improved products and services. Additionally, we believe the financial ecosystem benefits from increased competition, innovation, and consumer-driven business models.

While the consumer should have ultimate control over their data and useability, this clarification will allow consumers to permission their data to be used for the development of new and innovate products and services. ETA believes consumers should be able to consent to share their



data, however this must occur in a safe and secure environment and there must be certain provisions in place to maximize consumer awareness. With this in mind, it is vital that all data recipients 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.

For example, the CFPB could require data recipients to periodically reconfirm and re-obtain consumer authorization to access their accounts which would ensure that consumer data is not shared indefinitely.

### C. Standard-setting

A group of banks, data aggregators, and third-party providers established the Financial Data Exchange<sup>1</sup> (FDX) to unify the financial industry around a common, interoperable API standard for consumers and businesses to conveniently and securely access their financial data. These legacy processes like “screen scraping” that leave consumers exposed to risk and the CFPB should adopt technical standards that can securely move data from banks to aggregators and beyond, such as APIs, that allow for more secure transmission of data between systems in a standardized format. This empowers customers to share financial data without forfeiting their bank-user credentials. Additionally, having a mechanism for data traceability allows all parties receiving data downstream to see whether these parties can conduct fair practices. However, ETA cautions the CFPB from adopting FDX’s standard as the only standard but should adopt a broader-based standard-setting by system participants. This will ensure that the full ecosystem will be able to participate.

The CFPB should reference the U.K.’s Open Banking Standard.<sup>2</sup> The U.K.’s Standard goes beyond standard setting for the financial service providers to include standards for data holders as well. U.K. consumers will only use their Open Banking products and services if their experience matches or betters their expectations and information is present in an intuitive manner that allows them to make informed decisions. This has allowed their Standard to be implemented across 90% of the U.K. payments account market.

### D. 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.

The CFPB should affirm that Section 1033 will continue to give consumers control over their financial data, so that consumers continue to benefit from innovations. In addition, the CFPB should also address the U.S. Department of Treasury’s recommendation “that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data

---

<sup>1</sup> <https://financialdataexchange.org/>

<sup>2</sup> <https://standards.openbanking.org.uk/>

aggregators and consumer fintech application providers, fall within the definition of ‘consumer’ under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.”<sup>3</sup> 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.

#### E. Consumer control and privacy

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 raised concerns, including privacy, cybersecurity, liability, and safety and soundness of the financial sector. Given these 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 necessary 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 liability concerns before publishing a final rule. Data aggregators most commonly, have signed data access agreements with banks that transition from credentials-based data access to API-based access, but 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? 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 a data breach guide, similar in scope to the OCC’s Third-Party Guidance.<sup>4</sup> Any liability framework adopted by the CFPB should ensure that consumers are made whole in the event of a loss and provide a practical, efficient, and fair means to assign liability. We believe that this issue is extremely important and harmonization among consumers complaints needs to be fully addressed.

#### G. 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

---

<sup>3</sup> [https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation\\_0.pdf](https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf)

<sup>4</sup> <https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>

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 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. ETA supports a performance-based standard that allows for flexibility and innovation, rather than a prescriptive requirement that necessarily favors one method over another.

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. 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.

The CFPB should establish a control framework to set reasonable security standards for each class of entity. This framework should be implemented 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. Therefore, CFPB oversight into the data security practices of all entities would provide consistent protection for consumers and their financial data.

#### H. Data accuracy

Accurate data is important for all participants. Data aggregators depend on proper categorization to deliver experiences that improve consumers' lives. And their customers use this data to build experiences such as budgeting tools to even fraud analytics.

Apps for managing credit card points rely on merchant classification to suggest which card will provide the best deal. For most of these applications, accurate data is the difference between a delightful user experience and a product that simply doesn't work, and products won't deliver the value their users expect.

Open banking works best when consumer data is accurate. If data is incorrect, ETA encourages all parties to quickly and collectively work together and correct the data. ETA recommends the CFPB coordinate with other prudential regulators as well to ensure that the data is accurate.

\* \* \*

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](mailto:stalbott@electran.org).



Sincerely,



Jeff Patchen  
Manager of Government Affairs  
Electronic Transactions Association  
[jpatchen@electron.org](mailto:jpatchen@electron.org)  
(202) 677-7418

