ELECTRONIC TRANSACTIONS ASSOCIATION

1300 Connecticut Avenue, Suite 475
Washington, DC 20036

202.828.2635
electran.org

October 30, 2023

Via Email Submission

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

Re: Comments Regarding CFPB Proposed FCRA Rulemaking – SBREFA Proposals and Outlines

Dear Director Chopra:

On behalf of the Electronic Transactions Association (ETA), we appreciate the opportunity to share our thoughts in response to the Consumer Financial Protection Bureau's (CFPB) request for feedback during the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA) panel regarding the Fair Credit Reporting Act (FCRA) rulemaking.

ETA commends the CFPB's commitment through a process that invites input from the public and other stakeholders and welcomes the opportunity to be part of the dialogue. To that, ETA's members are dedicated to providing innovative, convenient, secure, and timely financial services and products that make their customers' lives easier.

ETA appreciates the opportunity to contribute to this important dialogue and remains committed to supporting efforts that promote fair, transparent, and competitive markets for consumer financial products and services. However, we urge the CFPB to carefully consider the impact of its proposals on fraud prevention and identity verification by financial institutions and in the payments and lending ecosystem holistically – including the potential impact this rulemaking will have on the Section 1033 proposal.

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.

ETA's Input on CFPB's SBREFA

The FCRA was specifically designed to regulate consumer reporting agencies and consumer reporting data users and address abuses within the industry. Its provisions focus on ensuring fair and equitable handling of consumer information, emphasizing confidentiality, accuracy, relevancy, and proper use.

The landscape of data collection and utilization has significantly evolved since the enactment of the FCRA, as the digital transformation and shift to online activities, including novel uses of consumer data such as consumer permissioned sharing with third-parties, identity verification and fraud prevention efforts by commercial enterprises, and ecommerce, has resulted in many more non-consumer reporting agency companies having access to data about their customers due merely to the fact that customers engage with their services through computer systems. While these companies have access to and use data

generated through these systems and in some cases share this data with third parties to benefit customers (e.g. sharing payment method information as a necessary stage of execution a transaction instructed by the customer, including the use of that data to run anti-fraud and anti-money laundering checks to reduce risk to the customer), it is crucial to acknowledge the different contexts and purposes in which they operate.

Entities Unknowingly Becoming Consumer Reporting Agency

As proposed in the Outline, the CFPB is considering treating entities that communicate consumer data to third-party recipients as a consumer reporting agency, even if they have no intention of producing consumer reports or sharing data for eligibility determinations.

According to the FCRA's definition of a "consumer reporting agency," an entity must be "regularly engaging" in the practice of assembling or evaluating consumer information for the "purpose of furnishing consumer reports" to third parties.[1] Under the CFPB's proposals, an entity could become a consumer reporting agency without knowledge or intent when a recipient uses data for eligibility purposes beyond the agreed-upon purposes. Even if the entity becomes aware of the misuse by a recipient, the entity – if not a consumer reporting agency – will likely not be prepared to commence full compliance with the significant obligations of that designation. It is not reasonable to expect them to do so when the underlying intent of the recipient is not known or otherwise disclosed. This becomes increasingly difficult if a recipient retains data for a significant period of time; while the initial data could have been used as agreed upon between the parties, it may be that a recipient, after maintaining data for a certain period of time, decided to use such data for eligibility or other purposes unknown to the providing entity. Further, other users of that same information could be impacted without their knowledge or time to plan for compliance associated with FCRA oversight, putting them at risk of violating the FCRA for using a consumer report if another information recipient uses the data for eligibility purposes. The scenarios above demonstrate only some of the potential outcomes that could occur if this significant expansion of "consumer reporting agency" becomes law.

To avoid these perverse consequences that are inconsistent with the FCRA, ETA recommends the CFPB should:

1. Clearly establish that a company does not become a consumer reporting agency merely because a third party with which the first company shares information in fact uses that information for eligibility purposes. In addition, the CFPB should provide an optional safe harbor affirmatively exempting a company that shares information under a contract that prohibits the recipient from using the information for eligibility purposes.

2. Clarify the terms "assembling" and "evaluating." Merely summarizing, or reiterating data about a consumer, even in a different format but without adding any insight or additional information, should not be considered "assembling" or "evaluating."

3. Preserve the mere passing of consumer information between entities via an intermediary outside the scope of a consumer reporting agency.

[1] 15 U.S. Code § 1681a

Interaction with Other Laws and Regulations

While the CFPB's proposal is silent as to whether providers of consumer information to data brokers may be considered "furnishers" under the FCRA, ETA believes it is important for the agency to answer and clarify if entities that provide data are subject to Section 1033 of the Dodd-Frank Act and other laws governing the sharing and usage of consumer data. This will ensure consistency and clarity and mitigate redundancy for impacted entities that engage in activities that overlap with these rules.

Financial Institutions, Lenders, Nonbanks, and Payment Companies Use Credit Header Data for Fraud Prevention, KYC, AML Prevention Purposes

Financial institutions, lenders, nonbanks, and payment companies use information such as name, address, and Social Security Number to verify consumer identity to protect consumers from third-party identity theft and identity fraud. This is not only a legal and regulatory requirement for all financial institutions, nonbanks or otherwise, but it is a necessary safeguard against the growing threat of fraud and identity theft consumers face every day. The CFPB should exclude the use of credit header data used in accordance with identity verification and fraud prevention to ensure entities that rely on such information can continue to use it in a lawful manner to protect their consumers, serve their communities, and meet their Customer Identification Program (CIP) and Anti-Money Laundering (AML) compliance obligations pursuant to the USA PATRIOT Act and Bank Secrecy Act, respectively.

Services for Fraud Prevention and Identity Verification are Critical to a Robust Payments Ecosystem

The use of verification services for fraud prevention and identity verification, which commonly rely upon credit header type and other data, is a key component of the payments ecosystem. Merchants, small businesses, and suppliers increasingly rely on verification services to identify legitimate prospective payments and identities of counterparties. In addition, a company that has data about a customer may share that data with a partner (either a third-party service provider to the company or a partner that has an independent customer relationship with the underlying consumer) for the purposes of combatting fraud; combatting money laundering, terrorist financing, or other financial crimes; supporting compliance with sanctions, and otherwise verifying customer identity – e.g., a customer with minimal transaction history may present a greater risk of fraud, and sharing the fact that a customer has such minimal history can better enable companies to identify bad actors and stop transactions from occurring that would otherwise result in economic loss to consumers.

In fact, the CFPB has encouraged payment providers to adopt tools to mitigate fraud during account activity to improve the overall safety and security of their products and services for consumers and the payments ecosystem.[2] These activities are not being undertaken for an FCRA purpose (i.e., determining eligibility for employment, credit, or insurance) but rather are attempts to evaluate payors and payees to facilitate payments and reduce fraud. These verification services necessitate the passing of data and use of basic details about accounts and individuals. Confirming account legitimacy or a counterparty's identity reduces returned payments, lowers operating costs, and hastens processing to consumers' benefit. While there is some intersection of this activity with the established consumer reporting agencies and some other data holders, expanding the scope of the FCRA to capture this activity would be a massive disruption to this growing Main Street business and could have the unintended impact of reducing consumer access to payment products and services. Specifically, if merchants and other billers cannot obtain some validation of accounts and account holders before making or accepting a payment to minimize potentially fraudulent

[2] See Office of Servicemember Affairs Annual Report January – December 2022

activity, they may well choose not to offer that method of payment to consumers at all, thus diminishing the payment options available to consumers.

As a result, the CFPB's proposed rule should include express exemptions for the sharing of data for anti-fraud; anti-money laundering, terrorist financing, or other financial crimes; sanctions; and identity verification purposes – as data shared for these purposes is clearly not a "consumer report" under the FCRA.

Request for Comment Period Extension and Consideration of Regulatory Alignment

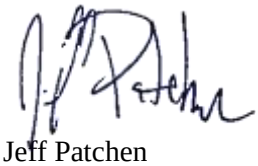
In line with the letter dated October 6, 2023, from ETA and other leading trade associations, we reiterate our request for extending the comment period, particularly due to the forthcoming Section 1033 proposal. Our members seek this extension to allow a thorough review of potential overlaps between the FCRA SBREFA materials and the proposed obligations in Section 1033 space. If the CFPB is unwilling to grant a full 90-day comment period for the FCRA SBREFA materials, we would ask for a minimum extension of 30 days from the release of the Section 1033 proposal.

Given the forthcoming Section 1033 rulemaking, the CFPB should remain cognizant of any potentially diverging or contradictory regulatory requirements that could emerge from the FCRA and Section 1033 reforms. Failure to account for these differences may undermine the competition principle consistently referenced by CFPB leadership and explicitly discussed in the Section 1033 SBREFA report.[3]

* * *

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

Sincerely,



Jeff Patchen
Director of Government Affairs
Electronic Transactions Association

[3] CFPB, *Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights*, (Washington, D.C., Mar. 30, 2023).