November 6, 2023

Just Futures Law SBREFA Comment Letter on Consumer Reporting Rulemaking

Just Futures Law and the undersigned public interest organizations appreciate the opportunity to comment on the Consumer Financial Protection Bureau's (CFPB) Small Business Regulatory Enforcement Fairness Act (SBREFA) outline concerning the pending rulemaking pursuant to the Fair Credit Reporting Act (FCRA). We write to respond to the data broker and big bank industries' argument that the outline of proposals under consideration, if made into a rule, will thwart its ability to prevent fraud to consumers. Specifically, in a recent article, the banking industry claims that requiring more data brokers to follow FCRA and limiting the sale of credit header data "could potentially be disrupting the ecosystems that banks and financial firms have built to prevent fraud and correctly verify the identity of customers." [1]

The industries' arguments are unfounded for the following two reasons:

1. **Businesses can still conduct identity verification and fraud prevention activities.**

Big business argues that restricting the sale of data to permissible purposes would mean "the use of data for identity verification to access a streaming service or an online account would be prohibited without a consumer's written authorization."

This is wrong. FCRA already permits the use of consumer reports to prevent fraud, and the proposals under consideration would not change that. Businesses may continue to obtain consumer data from furnishers under an existing permissible purpose under FCRA for legitimate business need.[2] If a bank's customer has initiated a transaction, by seeking to create an account with a particular company, like an online streaming service, nothing in FCRA or the proposals under consideration will limit that bank's ability to obtain consumer information as part of its fraud prevention efforts.

Moreover, if industry were required to obtain a consumer's written authorization, the burden of that additional step pales in comparison to the harms that consumers suffer under the status quo. Those harms include loss of access to credit, job opportunities, housing, and even increased risk of arrest and deportation.

---

[1] Kate Berry, "CFPB outlines sweeping data proposal, drawing swift bank condemnation," American Banker (Sept. 21, 2023), *available at* https://www.americanbanker.com/news/cfpb-outlines-sweeping-data-proposal-drawing-swift-bank-condemnation

[2] Section 1681b of FCRA provides that "any consumer reporting agency may furnish a consumer report under the following circumstances and no other…(F) otherwise has a legitimate business need for the information – (i) in connection with a business transaction that is initiated by the consumer; or (ii) to review an account to determine whether the consumer continues to meet the terms of the account."

Lastly, the banking industry argues that limiting the sale of credit header data would "impact a wide range of industries and companies including identity verification, fraud prevention firms and debt collectors." Here again, the industry's concerns are unfounded. If this proposal becomes a rule, banks would remain free to obtain this information from the credit bureaus and any data broker that complies with the FCRA's modest requirements: to offer consumers notice and an opportunity to dispute problems with their file.

In today's economy, businesses routinely use credit header data – some of which is inaccurate – to make decisions that impact people's access to shelter, work, essential utilities, and credit. People should have the right to know what information companies are using to inform these life-altering decisions; the right to protect their personal information from disclosure; and the right to dispute mistakes that impact their very livelihood.

Given the harm caused by misuse of credit header data, the proposed requirement is fair and warranted with minimum disruption to a well-resourced banking industry.

2. **The sale of credit header data and other data broker activity is itself a source of fraud and other criminal activity, including doxing, harassment, and potentially even physical violence.**

Because credit bureaus can sell credit header data, this data–which contains name, residential address, phone number and even Social Security Number information–has become readily available for purchase online. In the same article, the banking industry concedes that the unregulated trade in credit header data poses "concerns stemming from the use of this information by unscrupulous nonbank companies." Published reports have documented how this online marketplace for credit header data is used for doxing, identity theft, harassment, and even physical violence.[3] The sale of this sensitive personal data actually causes, rather than prevents, abuse and harm. This market cannot be allowed to flourish at the cost of personal safety.

[3] *See* Joseph Cox, 404 Media, "The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15" (Aug. 22, 2023), available at https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/ ("This is the result of a secret weapon criminals are selling access to online that appears to tap into an especially powerful set of data: the target's credit header. This is personal information that the credit bureaus Experian, Equifax, and TransUnion have on most adults in America via their credit cards. Through a complex web of agreements and purchases, that data trickles down from the credit bureaus to other companies who offer it to debt collectors, insurance companies, and law enforcement."); Hugh Aver, Kaspersky.com, "How to protect yourself from doxing," (Apr. 29, 2021), available at https://www.kaspersky.com/blog/doxing-methods/39651; Justin Sherman, "Data Brokers and Sensitive Data on U.S. Individuals," (2021), available at https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

We urge the CFPB to give due consideration to the interests of ordinary people, consumers, and small businesses, and issue the strongest possible protections to govern the sale of consumer data and the companies that profit from it.

Sincerely,

Laura Rivera
Just Futures Law

Ruth Susswein
Consumer Action

Jacinta González
Mijente

Jennifer Chien
Consumer Reports

Alli Finn
Surveillance Resistance Lab

Kate Oh
Demand Progress Education Fund

Akina Younge
UCLA Center on Race and Digital Justice

Caitlin Seeley George
Fight for the Future