November 1, 2023

Submitted Via Electronic Mail

Comment Intake
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, D.C. 20552
CFPB_consumerreporting_rulemaking@cfpb.gov

Re: Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration

To Whom It May Concern:

The Consumer First Coalition ("CFC") welcomes the opportunity to provide comments on the Consumer Financial Protection Bureau's ("Bureau") Small Business Regulatory Enforcement Fairness Act ("SBREFA") outline for the Consumer Reporting Rulemaking ("SBREFA Outline").

Established in 2018, the CFC represents a group of companies, both banks, non-banks, and service providers, committed to combatting new forms of fraud, protecting identities, and upholding the privacy protections that are a hallmark of the financial services industry. The CFC has led industry efforts to address synthetic identity fraud through implementation of the Social Security Administration's ("SSA") Electronic Consent Based SSN Verification System ("eCBSV"), pursuant to the 2018 Economic Growth, Regulatory Relief, and Consumer Protection Act. The eCBSV allows financial institutions and certain trusted third parties to verify through a real-time system whether a given name, date-of-birth and Social Security number on an application for a financial product are a match with what the SSA has on file. Additionally, the CFC is focused on other policy issues impacting fraud and identity protection in financial services. One such issue is preventing fraud in credit repair. Scammers often use the Fair Credit Reporting Act ("FCRA") credit dispute process to falsely claim errors or fraud in attempts to erase unpaid debt from a consumer's credit report, imposing costs on financial services firms and credit reporting agencies, undermining the integrity of credit underwriting, and causing substantial consumer harm.

Our comments on the SBREFA Outline are intended to further those goals – continuing to ensure that those in the financial services industry have the tools to combat fraud and protect consumers' identities. Specifically, CFC urges the Bureau to ensure that:

- Credit header data continues to be available for fraud detection and prevention and identity verification; and

- The consumer dispute process is robust, providing avenues for relief for consumers with safeguards to ensure bad actors do not take advantage.

Response to Questions 16-18

Credit header data is critical for fraud prevention and identity verification and should not be deemed a "consumer report" under the FCRA.

By law, regulation and supervisory guidance (e.g., BSA/AML law and regulations and the FFIEC's Consumer Identification Program), financial institutions are required to obtain identifying information about a potential customer and verify the customer's identity. This is to protect consumers against identity theft and fraudulent use of their identity to commit crimes, and safeguard the financial services system as a whole from illegal and fraudulent activity. This identity verification is performed before an evaluation for credit and also is done in non-credit transactions (e.g., a consumer requesting a deposit account). A common and effective tool for such identity verification is credit header data (which we typically define as the consumer's name, address, date of birth, and Social Security number).

The fact that financial institutions and their service providers use certain data for fraud prevention and identity verification purposes is well recognized under existing laws. For example, under the Gramm-Leach-Bliley Act, the notice and opt out requirements do not apply to the sharing of nonpublic personal information to "protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability."[1] Similarly, Section 1033 of the Consumer Financial Protection Act ("CFPA"), for which the Bureau recently issued a proposed rule, exempts any information collected "for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct" from the mandate to make information available to the consumer.[2] Similarly, and as acknowledged in the Bureau's recent advisory opinion on Section 1034(c) of the CFPA, financial institutions are not required to make available to the consumer any information collected by the institution "for the purpose of preventing fraud or money laundering, or detecting or making any report regarding other unlawful or potentially unlawful conduct."[3] The FCRA itself recognizes the necessity of identity verification. For example, when a consumer report includes an initial fraud alert or an active-duty alert, the FCRA requires a user of the consumer report to contact the consumer using a telephone number if indicated "or take reasonable steps to verify the consumer's identity and confirm that the application for a new credit plan is not the result of identity theft."[4]

[1] 15 U.S.C. § 6802(e)(3)(A) and 12 C.F.R. § 1016.15(a)(2)(ii).
[2] 12 U.S.C. § 5533(b)(2).
[3] 12 U.S.C. § 5534(c)(2)(B).
[4] 15 U.S.C. § 1681c-1(h)(B)(ii).

Merchants, small businesses and suppliers increasingly rely upon verification services to identify legitimate prospective payments and identities of counterparties. In fact, the Bureau has encouraged payment app 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 overall payments ecosystem.[5] 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 prior to making or accepting a payment, to otherwise minimize potential fraudulent activity, they may well choose to not offer that method of payment to consumers at all, thus diminishing the payment options available to consumers.

The Bureau must continue to acknowledge the importance and necessary differential treatment for information used for fraud prevention, identity verification and related activities. Classifying credit header data used for these purposes as a "consumer report" would conflict with financial institutions' existing obligations under state and federal law. Additionally, classifying credit header data as consumer reports would create substantial compliance challenges that would interfere with banks' ability to quickly and successfully combat and prevent fraud.

Moreover, such a classification would frustrate the purpose of fraud prevention and actually assist criminals. For example, if a criminal is attempting to open a line of credit under a stolen identity, and the use of credit header data for fraud prevention is considered a consumer report, then under the FCRA, the user of such information would be required to provide the criminal with an adverse action notice. The information in that adverse action notice could very well provide the fraudster with information on how their fraud is detected – essentially giving them critical information that they can then use to further perpetuate fraud. That is completely at odds with consumer protection and the goals of the Bureau. Additionally, the FCRA dispute process could allow criminals the opportunity to change a victim's contact information, further solidifying the fraudster's ownership and the consumer's victimhood.

[5] Office of Servicemember Affairs Annual Report January – December 2022.

Furthermore, it is unclear whether identity verification or fraud prevention would be a permissible purpose under the FCRA. If that is the case, banks would be hamstrung and unable to use this vital information to meet other legal obligations and prevent fraud. It may be that use for identity verification or fraud prevention may fall under two permissible purposes: "a credit transaction involving the consumer" or "a legitimate business need for the information… to review an account to determine whether the consumer continues to meet the terms of the account." This further supports why FCRA was never intended to cover fraud prevention activities.

The FCRA was never intended to cover financial institutions' fraud mitigation and identity verification activities, and to conclude otherwise would make it substantially difficult for such institutions to adhere to their legal obligations, detect and prevent fraud, and protect consumers. The Bureau should exclude the use of credit header data for identity verification and fraud prevention from coverage under FCRA.

Response to Questions 32 – 34

The consumer dispute process under the FCRA must be robust with appropriate safeguards. CFC and our members are committed to assisting victims of identity theft and fraud. We also want to be sure that consumers are not being taken advantage of and being charged by unscrupulous credit repair organizations ("CROs") that make false promises.

It is increasingly difficult to ascertain who is a victim of identity theft or fraud and who, either on their own or with the help of a predatory CRO, is falsely making claims of such victimhood. CROs filing illegitimate claims as they promise to help customers fix low credit scores for a substantially high fee clog the system and victimize not only the customers they claim they are helping, but also consumers that are trying to right actual wrongs committed against them.

Filing a fraudulent identity theft claim will remove (at least temporarily) the disputed information from the consumer's credit report while the claim is investigated. This is known as "credit washing," as the consumer's credit report and score look better than it actually is, at least temporarily. Removing such a disputed item when a factual claim is being made is appropriate. However, it is increasingly difficult, if not impossible, to ascertain true claims from fraud. As cited in a December 2022 Wall Street Journal article, lenders believe that 80-90% of the claims they receive about identity theft are fraudulent.[6] TransUnion reported that it received 1,200 letters supposedly from consumers in California, Massachusetts, and Virginia, all postmarked February 24, 2021, mailed from the same Pennsylvania ZIP code, and with the same

[6] Anna Maria Andriotis, Deluge of Fraud Claims Adds to Concerns about Credit Scores (Dec. 1, 2022).

format, text and typos. All claimed that a consumer had reached a settlement "to resolv" a debt on an account, which should "now be considered" paid off.[7]

The Bureau is well aware of the harm CROs can cause consumers. These entities claim they can help consumers invalidate, eliminate or lower their debt. Charging consumers initial fees and ongoing monthly fees (e.g., $89.99/month), these organizations, often unbeknownst to the consumer, repeatedly file false credit disputes and claims of identity theft to the credit bureaus. The most common result is the consumer's valid debt is not eliminated and the only success the organization had is in fraudulently obtaining hundreds, if not thousands, of dollars from unsuspecting consumers. Consumers are paying hundreds of dollars a month and not receiving any meaningful assistance. If a false credit dispute or identity theft claim is filed, it may result in a temporary, but not permanent, boost in the consumers credit score. According to the Bureau, there are as many as 46,000 businesses that offer credit repair services in the U.S. – the vast majority of which are sole proprietorships.[8] The Bureau sued Progrexion (aka Lexington Law) alleging that, over a 7-year period, Lexington Law took approximately $3.1 billion from more than 4 million consumers in violation of the Telemarketing Sales Rule as well as engaging in deceptive marketing.[9] Lexington Law ultimately filed for bankruptcy and agreed to a settlement imposing a $2.7 billion judgment on it, along with a ban from telemarketing credit repair services for 10 years.

Our members are seeing this firsthand. According to some CFC members, the volume of disputes filed without supporting documentation doubled between 2019 and 2022, and most saw a decrease in disputes with supporting documentation. While documentation is not a requirement, it is often an indication of whether the claim is legitimate.

CFC is concerned that providing consumers (and those working on their behalf) with a specific process through which they could notify a consumer reporting agency or furnisher of possible systemic consumer reporting issues will only further clog the dispute resolution process and lead to an increase in fraudulent claims. To be clear, our members are committed to ensuring that true victims get the assistance they need and are not negatively impacted. We fear that the proposal the Bureau is contemplating will frustrate that goal and only help fraudsters, not true victims.

Individual consumers are not well positioned to identify systemic errors, whereas data furnishers are in the best position to identify and resolve furnishing errors. Existing law requires furnishers to update and correct reporting inaccuracies after discovery, and consumers

[7] Id.
[8] Source: CFPB Annual Report on Credit Reporting Consumer Complaints, Jan. 2022.
[9] https://www.consumerfinance.gov/about-us/newsroom/bureau-files-suit-against-lexington-law-pgx-holdings-and-related-entities/; https://www.accountsrecovery.net/wp-content/uploads/2023/04/CFPB-v.-Progrexion-et-al.pdf.

who are impacted are notified by updates to their credit report. Sending an additional notification could be confusing to consumers and would also create an avenue for further abuse by dishonest CROs without benefiting consumers or improving accuracy of credit reporting.

Instead, the identification, investigation, and remediation of any systemic consumer reporting issues is best left to the examination and supervision function by the Bureau and other relevant supervisory authorities (e.g., prudential banking agencies).

In conclusion, the CFC reiterates its appreciation for the opportunity to provide comments on the SBREFA Outline and encourages the Bureau to: (1) ensure the financial services industry can continue to use credit header data as a tool against fraud and identity theft; and (2) avoid enabling bad actors further opportunity to take advantage of consumers under the auspices of credit repair.

Thank you for considering these comments. If you have any questions, please contact Katie Wechsler, kwechsler@snwlawfirm.com.

Sincerely,

Katie Wechsler
Co-Executive Director
Consumer First Coalition