September 5, 2023

Via Electronic Mail

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

Re: Forthcoming CFPB "Data Broker" Rulemaking under the FCRA

To Whom it May Concern:

The Consumer Bankers Association ("CBA")[1] sends this letter in response to the Consumer Financial Protection Bureau ("CFPB" or "Bureau") Director Rohit Chopra's remarks at the White House Roundtable on Protecting Americans from Harmful Data Broker Practices and additional details[2] released on the scope of CFPB's forthcoming Small Business and Regulatory Enforcement and Fairness Act ("SBREFA") outline and Notice of Proposed Rulemaking (NPRM) related to data brokers under the Fair Credit Reporting Act ("FCRA") and Regulation V.

CBA understands that, as part of the forthcoming rule related to the FCRA and Regulation V, the Bureau intends to:

- Prohibit firms that monetize certain data from selling it for purposes other than those authorized under the FCRA.
- Broaden the scope of a consumer reporting agency to include a data broker or other company in the surveillance industry.
- Clarify the extent to which "credit header data" constitutes a consumer report and prevent the sale of this type of data for a reason other than a "permissible purpose."

CBA shares the Bureau's concern over consumer data used for purposes that pose risks to consumers. As the Bureau undertakes this effort, CBA would like to provide some insight on the consumer protective ways that banks use credit header data. We ask that the Bureau give

[1] CBA is the only national trade association focused exclusively on retail banking. Established in 1919, the association is a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly $3 trillion in consumer loans, and provide $270 billion in small business loans.

[2] Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices (Aug. 15, 2023), *available at* https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/; *see also* Consumer Financial Protection Bureau, *Protecting the Public from Data Brokers in the Surveillance Industry* (Aug. 15, 2023), *available at* https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb-data-broker-rulemaking-faq_2023-08.pdf.

appropriate thought and consideration to the impact of any future rulemaking on these consumer protection activities.

Consumer Identity Verification

Banks are required under the Bank Secrecy Act[3] and the Federal Financial Institutions Examination Council's Consumer Identification Program[4] to obtain identifying information about a potential customer and verify the customer's identity. These laws and procedures protect consumers against identity theft and the fraudulent use of their identity to open accounts or commit crimes, such as initiating fraudulent electronic payment transfers. One of the tools banks use to verify consumer identities is information from companies (frequently credit reporting companies) that specialize in providing consumer identification information, which may include a consumer's first and last name, address, and social security number. Consumer identity information used by banks for identity verification purposes is currently protected and regulated under the Gramm-Leach-Bliley Act ("GLBA") and Regulation P. CBA understands that information used for identity verification may fall under the Bureau's forthcoming definition of "credit header data" and therefore may be considered a consumer report. If this information is considered a consumer report, it would then be subject to FCRA provisions including accuracy standards, permissible purpose restrictions, as well as the adverse action notice and dispute provisions.

Subjecting these routine – and statutorily required - consumer identity verification practices to the FCRA would substantially increase a bank's compliance obligations and potentially create consumer confusion (for example, if a bank cannot confirm an individual's identity, would it be appropriate to send a notice to an individual whose identity cannot be verified?). This associated increase in compliance burden and costs could increase the price of credit or the cost for consumers to open an account. Further, it is unclear under the current FCRA statutory text whether account opening identity verification requirements are a "permissible purpose."[5]

Fraud Prevention

For years banks have been on the front lines fighting fraud and continue to do so in response to increasingly prevalent and sophisticated financial scams, including those across peer-to-peer (P2P) payment platforms. These actions include preventing, detecting, and mitigating fraud through monitoring and the use of transaction and consumer authentication tools. Financial

[3] 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951-1960, 31 U.S.C. §§ 5311-5314, §§ 5316-5336.

[4] 31 C.F.R. § 1020.220(a).

[5] Identity verification could fall under 15 U.S.C. § 1681b(a)(3)(A) as activities involving "a credit transaction involving the consumer… and involving the extension of credit to, or review or collection an account of, the consumer." It may also fall under the "catch-all" provision in 15 U.S.C. § 1681b(a)(3)(F) as "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." However, the scope of any "permissible purpose" for these actions is unclear and would require explicit regulatory clarification and confirmation.

institutions also play an important part in preventing money laundering, the financing of terrorism, and crime. Additionally, when a consumer report includes an initial fraud alert or an active-duty alert, the FCRA requires banks to verify the identity of a that customer before opening an account.[6] Being able to confirm identifying information about a consumer, which may be considered "credit header data," is critical—and required by law—to those responsibilities.

Subjecting information used to investigate fraudulent activity to the FCRA could create compliance challenges and hurdles where time is of the essence to stop the fraudulent activity and protect their customers (for example, a receiving bank's investigation into a potential P2P payment fraud or scam). FCRA could create additional compliance burdens for banks when investigating fraud through increased liability for potential consumer disputes, the requirement to issue adverse action notices which must indicate how "credit header data" was used (which may tip off fraudsters to bank prevention practices), and timing delays inherent in having to proactively identify a "permissible purpose" prior to accessing the data. Fraudsters could also dispute credit header data as a means to circumvent fraud prevention. Further, similar to identity verification purposes, it is unclear under the current FCRA statutory text whether account opening and payment processing identity verification requirements are a "permissible purpose."[7]

Conclusion

CBA's member banks spend millions to protect their consumers from fraud and identity theft and want to ensure that they are able to carry out these vital functions without substantial increased compliance burden and costs. We urge the Bureau to consider the ways that banks use "credit header data" when crafting the scope of the forthcoming FCRA rulemaking - including possibly excluding the use of credit header data by banks for identity verification and fraud prevention from coverage under FCRA - to ensure that CBA's member banks can continue to use consumer information in lawful and responsible ways to protect their consumers and serve their communities.

We look forward to reviewing and providing industry expertise in comments on the Bureau's future SBREFA outline and NPRM on Regulation V. Please do not hesitate to reach out with questions or if it would be helpful to have additional conversations with CBA or our member banks.

[6] Under 15 U.S.C. § 1681c-1, users of consumer reports may not extend credit, issue an additional card on a credit card account, or increase a credit limit without verifying the identity of the person making the request.

[7] The use of "credit header data" for fraud prevention may fall under 15 U.S.C. § 1681b(a)(3) as activities involving "a credit transaction involving the consumer." It may also fall under the "catch-all" provision in 15 U.S.C. § 1681b(a)(3)(F) as "a legitimate business need for the information (ii) to review an account to determine whether the consumer continues to meet the terms of the account." However, the scope of any "permissible purpose" for these actions is unclear and would require explicit regulatory clarification and confirmation.

Sincerely,

Shelley Thompson
Vice President, Associate General Counsel
Consumer Bankers Association