March 3, 2025

Consumer Financial Protection Bureau
1700 G St. NW
Washington, DC 20552

Re: Docket No. CFPB-2024-0044 – Protecting Americans from Harmful Data Broker Practices (Regulation V)

The Computer & Communications Industry Association (CCIA)[1] is pleased to respond to the Consumer Financial Protection Bureau's proposed Rule on Protecting Americans from Harmful Data Broker Practices ("the proposed Rules"). CCIA supports appropriate regulation to protect both consumers and businesses and greater protection of consumer data. However, we believe the proposed Rule exceeds the scope of FCRA and is unconstitutional. Both FCRA's statutory text and Circuit Court case law interpreting FCRA indicate that the proposed Rule is contrary to established law. Moreover, the proposed Rule does not show a consumer benefit that is commensurate with the regulatory burdens it places on businesses. CCIA therefore urges CFPB to withdraw the proposed Rule for the following reasons:

The proposed Rule attempts to regulate national security concerns more appropriately left to other agencies.

The proposed rule highlights various national security risks from foreign adversaries accessing the personal data of military and government personnel and using the information for coercion or espionage.[2] While mitigating such threats is of paramount importance, FCRA is the wrong vehicle for addressing national security concerns. Such concerns should instead be addressed using existing national security laws and regulations, such as the DOJ's export control laws or its recent rule on the transfer of bulk sensitive data to countries of concern.

Moreover, the proposed Rule uses these national security concerns to justify broad restrictions on the use of consumer data for identity verification, and fraud prevention. These measures would inhibit businesses' ability to use best practices to secure their customers' data, and would therefore compromise the very security that the proposed Rule aims to bolster. Furthermore, the proposed Rule uses such concerns to restrict product development, website personalization, advertising, and training model development, areas which lack any logical connection to the stated national security concerns. CCIA instead recommends allowing those agencies tasked with assessing national security threats to establish guidelines concerning the associated risks.

The proposed Rule would broaden the definitions of "consumer report" and "consumer reporting agency" beyond what is legally permissible.

The proposed rule would expand the definition of "consumer report" to include any information collected about a consumer's income, wealth, debt payments, or credit scores and history from

[1] CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: https://www.ccianet.org/about.
[2] 89 Fed. Reg. at 101405 and 101411-412.

third parties, regardless of purpose. Accordingly, under this Rule, such information could only be obtained and used for FCRA permissible purposes, e.g. extending credit or insurance to consumers for personal, family, or household purposes, employment purposes, opening a bank account, or renting an apartment. If this information is used for other purposes, such as creating back-end internal models or detecting crime and fraud, the proposed Rule appears to treat the collecting entity as a consumer reporting agency.

This broadening of the definition of "consumer report" contravenes the statutory text, case law, and regulatory guidelines. FCRA requires that a "consumer report" be used, expected to be used, or collected for the "purpose" of establishing a consumer's eligibility for a FCRA permissible purpose.[3] Likewise, a "consumer reporting agency" must provide consumer information for the "purpose" of furnishing consumer reports to third parties.[4] These definitions are affirmed by both U.S. circuit court cases[5] and decades of regulatory guidance.[6]

The expanded definitions of "consumer report" and "consumer reporting agency" would inhibit business's efforts to improve their products and services.

There are good policy reasons not to broaden these definitions. Businesses regularly conduct research and build models to develop and improve their products and services. For products and services designed for consumers within certain income ranges, such research and modeling frequently are based on consumer financial data. While it is important that consumer privacy be protected during such uses, the proposed rules would prohibit businesses from obtaining and using even de-identified or aggregated income or financial tier data from third-party sources. Under the proposed Rules, such sources would be considered consumer reporting agencies, and product development is not a permitted purpose under FCRA.

Product and service personalization could suffer as well. For example, loyalty programs require businesses to personalize their products and services for frequent customers, sometimes based on the above categories of financial information. For instance, airlines may reward customers with airline miles for using their co-branded credit cards, which would require accessing customers' credit scores and history. However, the proposed Rule would prohibit airlines from obtaining and using such information because product personalization is not a permissible purpose under FCRA.

Even more troublingly, the proposed Rule undermines a key method of ensuring compliance with antidiscrimination regulations. Many businesses use risk models (often AI-based) to approve loans, credit card applications, or other financial products and services. When doing

[3] 15 U.S.C. § 1681a(d)(1).
[4] *Id.* § 1681a(f).
[5] *See, e.g.*, Kidd v. Thomson Reuters Corp., 925 F.3d 99 (2d Cir. 2019); Zabriskie v. Federal Nat'l Mortg. Assn., 940 F.3d 1022 (9th Cir. 2019).
[6] FTC Commentary on the Fair Credit Reporting Act, 55 Fed. Reg. 18808 at App. A, § 603(d)-3.A (May 4, 1990) ("A 'consumer report' is a report on a 'consumer' to be used for certain purposes involving that consumer,") (emphasis added); *id.* at § 603(f)-1.B ("The term 'consumer reporting agency,' . . . , includes certain persons who assemble or evaluate information on individuals for the purpose of furnishing 'consumer reports' to third parties.") (emphasis added). The FTC Commentary was rescinded and replaced the FTC Staff Report, *40 Years of Experience with the Fair Credit Reporting Act* (July 2011) ("*40 Years Report*"). The *40 Years Report* retained and expanded upon the existing interpretations of "purpose." See FTC, *40 Years Report* at 20 (Section 603(d)-5.A) and 30-31 (Section 603(f)-4.A-J).

so, they must comply with fair lending and labor laws such as the Equal Credit Opportunity Act, Fair Housing Act, and Equal Employment Opportunity Act. To ensure compliance, a model's developers will often check its recommendations against data from third-party sources to ensure that the model is not discriminating against a protected class of consumers. However, the proposed rule may prohibit this practice, leaving consumers more vulnerable to lending and housing discrimination.

The proposed Rule does not show any compensating advantage of this proposed change. CCIA appreciates CFPB's stated desire to mitigate harm from low-income consumers being targeted with "predatory" products,[7] but the Rule provides no data on the frequency or cost of such harms and does not further define "predatory" products. The Rule also does not explain why combatting such harms can only be done using sweeping restrictions on the ability of legitimate businesses to process data in ways that benefit consumers.

Credit header data should not be treated as a "consumer report."

The proposed rule would treat contact and identification information collected by a consumer reporting agency as a consumer report, even when such information is not associated with any factor used to evaluate creditworthiness. These personal identifiers are known as "credit header data." The proposed rule would prohibit companies from acquiring this non-financial, credit header data from consumer reporting agencies for non-FCRA purposes. Such a restriction is contrary to established law and makes little sense from a policy perspective.

Many courts have recognized that credit header data is not "consumer report" information under FCRA since it does not "bear on a consumer's" creditworthiness or other personal characteristics and it is not used or expected to be used for the purpose of determining credit eligibility, employment or other FCRA purposes.[8] Long-standing agency interpretations concur with this conclusion.[9] The proposed Rule contradicts 50 years of legal precedent.

Furthermore, restricting credit header data sales would greatly disadvantage consumers, businesses, and government regulators. These groups all use credit header data from consumer reporting agencies for legitimate non-FCRA purposes like identity verification and

[7] *See* 89 Fed. Reg. at 101402, 101405, 101408, 10436-37, 101443, 101447.

[8] *See, e.g.*, *In re Equifax Inc., Consumer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1313 (N.D. Ga. 2019) (holding that "header information" is not a "consumer report" because it does not bear on an individual's creditworthiness); *Accord Harrington v. ChoicePoint Inc.*, No. CV 05-01294 MRP (JWJx), slip op. at 11-12 (C.D. Cal. Oct. 11, 2006); *Individual Reference Servs. Group, Inc. v. FTC*, 145 F. Supp. 2d 6, 17 (D.D.C. 2001); *Dotzler v. Perot*, 914 F. Supp. 328, 330 (E.D. Mo. 1996) (holding that a report containing plaintiffs' names, current and former addresses, and SSN does not "bear on plaintiffs' credit or general character and was not used to establish their eligibility for credit, employment or any of the other purposes listed in [FCRA]"); *Weiss v. Equifax, Inc.*, No. 20-cv-1460, 2020 WL 3840981 (E.D.N.Y. July 8, 2020) (holding that personally identifiable information stolen during a data breach is not a "consumer report" within the meaning of the FCRA); *Williams-Steele v. TransUnion*, No. 12 Civ. 0310 (GBD) (JCF), 2014 WL 1407670, at *4 (S.D.N.Y. Apr. 11, 2014) ("Neither a missing area code nor an allegedly inaccurate alternate address bear on any of the factors listed in 15 U.S.C. § 1681a(d)(1), or is likely to be used in determining eligibility for any credit-related purpose . . . ."); *Ali v. Vikar Mgmt., Ltd.*, 994 F. Supp. 492, 497 (S.D.N.Y. 1998) (holding that address information does not bear on factors); *Smith v. Waverly Partners, LLC*, No. 3:10-CV-28, 2011 WL 3564427, at *1 (W.D.N.C. Aug. 12, 2011) (holding that "[the defendant] did not communicate any information bearing on Plaintiff's 'credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living' . . . . Instead, it merely provided name, Social Security Number, prior addresses, date of birth, and driver's license information. Such minimal information does not bear on any of the seven enumerated factors in § 1681a(d) and is thus not a consumer report").

[9] FTC 40 Years Report at 21 ("[A] report limited to identifying information ... does not in itself constitute a consumer report if it does not bear on any of the seven factors."); *In the Matter of TransUnion Corp.*, FTC Docket No. 9255 at 30 (Feb. 10, 2000) (holding that name, SSN, and phone number of the consumer are not subject to the FCRA because they "[do] not ... bear on creditworthiness, credit capacity, credit standing, character, general reputation, personal characteristics, or mode of living, unless such terms are given an impermissibly broad meaning").

fraud detection and prevention. Such verification allows consumers to receive products and services quickly and efficiently, and allows businesses and governments to prevent fraud, theft, and unauthorized access to data. The Small Business Review Panel highlighted these very concerns in recent recommendations.[10]

Often, rather than provide the credit header data directly to the verifying business or official, consumer reporting agencies will provide the data to a third party which specializes in identity verification and/or fraud prevention. However, under the proposed Rule, third-party specialists would be unable to purchase credit header data to include in identity verification and fraud detection tools unless it provides such tools only to users with a FCRA permissible purpose. Even then, the third party would be labelled a consumer reporting agency that "furnish[es]" consumer reports under the proposed Rule, even if it does not provide the credit header data to its end user customers, as it facilitates merchants' use of the credit header data for financial gain. Note that FCRA's permissible purposes do not explicitly include identity verification, unless such activities are associated with a permissible purpose such as credit underwriting or written instructions of the consumer.

It is not easy to effectively replace the role of credit header data in identity and fraud checks: it is widely viewed as the most accurate and current source of identification, address, and other contact information. When consumers change their name or address, their bank is among the first entities they contact, to ensure that they continue receiving bank statements and bills. Banks also collect reliable identification information, such as SSN, when their customers open accounts. For these reasons, credit header data is often considered the most reliable and up-to-date identification method.

Similarly, FCRA's permissible purposes do not include fraud detection and prevention, unless such activities are associated with a permissible purpose such as credit underwriting or written instructions of the consumer. The proposed rule assumes that entities obtaining and using personal identifiers from consumer reporting agencies will have permissible purposes such as processing a consumer's loan application, or can obtain the consumer's written consent.[11] However, as explained above, these assumptions do not hold given the many uses for identity verification and fraud prevention tools beyond FCRA's permissible purposes. For these reasons, any final rule should not treat credit header data as consumer reports.

The proposed rules risk encompassing most digital advertising providers.

The proposed rule could result in digital advertising providers getting classified as consumer reporting agencies, since they routinely use financial data to determine which ads to market to particular audiences and then "furnish" this information to advertisers for financial gain. It is not feasible for digital advertising providers to meet these requirements since advertising generally is not a FCRA permissible purpose. Instead, digital advertising providers would be unlikely to offer income-relevant targeted advertisements. This result would follow from two aspects of the proposal.

This policy directly contravenes the statutory text. As noted above, FCRA does not permit certain types of data to be inherently classified as a "consumer report"– such determinations

[10] 89 Fed. Reg. at 101418.
[11] *Id.* at 101419, 101441.

must be based on the purpose for which the data is used, expected to be used, or collected. The financial data advertising providers collect enables low-income consumers and other vulnerable populations to receive information on how to access consumer staples such as food and clothing, receive discounted products and services, and access government programs. Disregarding the "purpose" element of the definitions of "consumer report" and "consumer reporting agency" makes much of the proposed rule not only contrary to law but detrimental to many vulnerable groups of consumers.

Likewise, the proposed rules' criteria for when consumer reporting agencies "furnish" consumer reports is inconsistent with FCRA. Under FCRA, a "consumer report" requires a "communication" of information by a consumer reporting agency.[12] Without such "communication," there is no "consumer report" or "consumer reporting agency." Therefore, digital advertising providers cannot be considered consumer reporting agencies unless they furnish consumer reports to third parties. Any final rule should apply only to cases where an entity conveys the underlying consumer data to a third party.

* * * * *

We appreciate the CFPB's consideration of these comments. We look forward to continuing to participate in the regulatory process, including reviewing and providing feedback on proposed Rules. We hope CFPB will consider CCIA a resource as these discussions progress.

Sincerely,

Jesse Lieberfeld
Policy Counsel– Privacy, Security, and Emerging Technologies
Computer & Communications Industry Association

[12] 15 U.S.C. § 1681a(d)(1).