Submitted electronically
March 31, 2025

Consumer Financial Protection Bureau
Comment Intake—Protecting Americans from Harmful
Data Broker Practices (Regulation V)
c/o Legal Division Docket Manager
1700 G Street N.W.
Washington, D.C. 20552

FTA Comment Letter on the CFPB's Protecting Americans From Harmful Data Broker Practices Proposal (Regulation V) (Docket No. CFPB–2024–0044 or RIN 3170–AB27)

The Financial Technology Association ("FTA") is writing to raise concerns with the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") proposed rule amending Regulation V, which implements the Fair Credit Reporting Act ("Proposal").[1] As we have previously raised in multiple comment letters,[2] the CFPB's interpretations in this rulemaking effort go well beyond the statute's mandate and could be harmful to financial institutions' efforts to detect and prevent fraud.

FTA believes that consumer choice, trust, and protection are the cornerstone of financial services and that consumers are entitled to high levels of data stewardship from companies when sharing their personal financial information. A core pillar of FTA's effort to advance consumer-centric financial services development in the U.S. is advocating for modern regulatory frameworks that recognize and foster the benefits of financial technology-driven innovation and accommodate new models within the regulatory perimeter. To this end, FTA's members include furnishers and users of consumer report information that will be negatively affected if this Proposal is finalized as drafted. Therefore, we encourage the Bureau to withdraw and review this Proposal in line with President Trump's January 20, 2025 "Regulatory Freeze Pending Review" Directive.[3] Below are our key concerns with the proposed rule.

[1] 89 Fed. Reg.101402.
[2] *See* Financial Technology Association, "FTA Comment on the CFPB's Outline of Proposals and Alternatives Under Consideration Related to the Consumer Reporting Rulemaking" (hereafter FTA October 2023 SBREFA Letter) (October 30, 2023), available at https://www.ftassociation.org/wp-content/uploads/2023/10/FTA-Data-Broker_FCRA-SBREFA-Response-Letter-vF.pdf. *See also* Financial Technology Association, "FTA Comment on CFPB Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information" (July 14, 2023), available at https://www.ftassociation.org/wp-content/uploads/2023/07/FTA-Comment-Letter-re-Data-Broker-RFI.pdf.
[3] 90 Fed. Reg. 8249.

- **Fraud Prevention Tools Used Throughout the Industry Will Be Impacted by This Proposal and its Expansion of Dispute Rights.** The Proposal continues to inappropriately determine that credit header data constitutes a consumer report, which not only has no basis under the FCRA, but will also meaningfully impede efforts to combat fraud and abuse - notwithstanding the Bureau's comments to the contrary. For example, fraud models are tuned based on this data to identify potential fraudulent actors. When these services are used, they return scores based on usage, velocity, and other factors that may indicate that the applicant is a fraudster. If this data were to be covered under the FCRA, coupled with customer dispute rights, it would have a detrimental impact on fraud models. These models are built to be dynamic over time and evolve as risks change, leveraging "credit header" data. In addition, the enhanced dispute mechanisms would give fraudsters the ability to "cleanse" data they have purchased for continued re-use. As a practical matter, there is no alternative source of data to turn to for the purpose of a reliable identity match and these provisions should be removed from any future rulemaking.[4]

- **Consumer-Permissioned Data Sharing Should Not be Considered "Assembling or Evaluating" Under the FCRA as it is Communicated by a Consumer, Not a Consumer Reporting Agency.** The Bureau's Proposal continues to consider consumer-permissioned sharing, in certain instances, as covered by the FCRA's "assembling or evaluating" prong. Section 603(d)(1) of the FCRA defines consumer report, in part, as a "communication of . . . information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living." Consumer-permissioned data, such as data transmitted by entities operating as a consumer's "agent, trustee, or representative" pursuant to Section 1002 of the Consumer Financial Protection Act of 2010, are communications "by" the consumer. Because a consumer is not and cannot be a consumer reporting agency when transmitting their own information, the communication is not, and cannot under the FCRA definition be, a consumer report. Consumer-permissioned sharing is a critical component of the U.S. economy and allows fintech companies to offer consumers tailored and improved services. It is also an important tool for increasing access to credit through identity verification, and can facilitate no-fee salary advances, while safeguarding the financial system through enhanced fraud mitigation tools facilitated by robust identity verification capabilities. However, even after finalizing the Dodd-Frank Act's Section 1033 rule, the Bureau continues to improperly consider certain activities undertaken by data aggregators as covered under this rule. We believe that the definition of "assembling" should be tailored to achieve the FCRA's purpose of ensuring data accuracy in the context of credit reporting, and explicitly recognize that consumer-permissioned sharing of financial data is not covered.

[4] *See* FTA October 2023 SBREFA Letter for more information.

- **De-identified Data Should Not Be Considered a Consumer Report and is Currently Used for Pro-Consumer Purposes.** While the Proposal provides additional details relating to the sharing of de-identified data, none of the options provided goes far enough in facilitating the long-standing practice of sharing de-identified information. Financial service providers use de-identified consumer data to build more accurate credit underwriting models that foster a more inclusive credit ecosystem, among other things. It is also common for providers to securely share de-identified or anonymized data amongst themselves or consumer reporting agencies ("CRAs") for modeling, prescreening, product development, or portfolio evaluation purposes. If CRAs or other providers begin withholding such data, the quality of product offerings and underwriting models may suffer and negatively impact access to products for consumers, especially those who have limited access to credit already. While the Bureau proposes three options for treatment of de-identified data, absent a full exemption it will undo years of progress in creating a more inclusive credit ecosystem and risk leaving consumers with less access to credit.

- **The Proposal's Requirements Around Written Instructions and Separate Authorizations Will Add Additional Friction to Products and Services.** The Proposal's prescriptive requirements around written instructions will introduce even more consumer notices and will likely cause additional confusion as consumers may not realize the impact of providing multiple consents for each distinct product or service a platform provides. For example, customers commonly sign up for multiple products and services within a platform ecosystem, and the proposed rule would require the consumer to provide written instructions for *each* service. Additionally, the Proposal's requirement for such written instructions to be refreshed annually would be burdensome for platform users, which could inadvertently lead to disruptions in service. While we support the desired outcomes of transparency and express consent, we believe any future agency actions should allow flexibility around how a consumer's written instructions are obtained so that it is not overly burdensome or confusing and does not discourage the consumer from completing the desired activity.

- **Any Future Action Should Account for the Various Data-Related Frameworks Already in Place.** Lack of cohesion and consistency across and between relevant rules dealing with the treatment and use of data could result in confusion, uncertainty, duplication and gaps. This is particularly true in light of the CFPB's finalization of its open banking rulemaking under Section 1033. Government agencies have long recognized a separation between data brokers and other types of entities and have adopted narrower definitions of data broker than are set forth in the Proposal – including in California and Vermont. We believe the CFPB should take

a similar approach in any future rulemaking.[5] Separately, the Department of Justice's "Preventing Access to U.S. Sensitive Personal Data and Government Related Data by Countries of Concern or Covered Persons"[6] final rule holistically addresses national security concerns related to international bulk data transfers so any additional rulemakings under the FCRA would be unnecessary and redundant.

We appreciate your consideration of our concerns and would be happy to discuss anything raised in this letter with you further. More generally, we encourage you to halt this rulemaking effort as it would affect a broad spectrum of financial technology companies. Please reach out to me at penny@ftassociation.org with any questions.

Sincerely,

Penny Lee
President and Chief Executive Officer
Financial Technology Association

[5] For example, in California, "data broker" refers to a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. *See* Cal. Civ. Code § 1798.99.80. "Data broker" does not include any of the following: (1) A consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.); (2) A financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106- 102) and implementing regulations; and (3) An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code). In Vermont, a "data broker" is a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. See 9 V.S.A. § 2430. The definition expressly excludes entities that engage in developing or maintaining third-party e-commerce or application platforms or providing publicly available information related to a consumer's business or profession. It also excludes any one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or a sale or license of data that is merely incidental to the business.

[6] 90 Fed. Reg. 1636.