Comments of the Software & Information Industry Association

Consumer Financial Protection Bureau
Protecting Americans from Harmful Data Broker Practices (Regulation V)

April 2, 2025

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide feedback on the Consumer Financial Protection Bureau's (CFPB's) Proposed Rule to amend Regulation V.[1] As reflected below, our comments support the withdrawal of the Proposed Rule because it goes beyond the purpose and authorization granted to the Bureau by the Fair Credit Reporting Act (FCRA), and because it would lead to a host of severe unintended consequences.

SIIA is the principal trade association for those in the business of information. SIIA represents over 380 companies in academic publishing, education technology, financial information, software, platforms used by millions worldwide, and data analytics and information services. Our mission is to protect the three prongs of a healthy information environment essential to that business: creation, dissemination and productive use.

The Proposed Rule introduces data brokers, broadly, as "entities that collect, aggregate, sell, resell, license, enable the use of, or otherwise share consumer information with other parties."[2] Companies that fall into this definition publish information ranging from business-to-business news, to securities pricing, to databases of case law and other public records, to scientific, technical and medical articles. These publications are used for purposes ranging from academic research to corporate due diligence, and provide the building blocks of ideas: the backbone of functioning markets and a functioning democracy. Further, this information routinely helps both businesses and government deter, prevent, and track down fraudulent criminal activity.

Unfortunately, the Proposed Rule's broad approach to and understanding of data brokers, and even broader proposed categories of "consumer reporting agencies" and "consumer reports," would wrap in an unprecedented number of these entities whose activities are not consumer reporting based on any common understanding of the term. As detailed in this submission, we believe this expansion of the scope of the FCRA to cover functions that are socially beneficial, essential to the functioning of the internet, and have nothing to do with credit reporting or consumer reports will have significant harmful consequences for the U.S. economy. Further, the proposed expansion has no basis in current case law, agency interpretations, or Congressional intent.

[1] Consumer Financial Protection Bureau, *Protecting Americans from Harmful Data Broker Practices (Regulation V)*, Docket No. CFPB–2024– 0044, 89 Fed. Reg. 240, 101402 (Dec. 13, 2024), https://www.govinfo.gov/content/pkg/FR-2024-12-13/pdf/2024-28690.pdf.
[2] *Id.* at 101404.

1. **The Proposed Rule's definition of "consumer report" is overbroad and not supported by current caselaw, agency interpretations or congressional intent. It would designate a host of entities as "consumer reporting agencies" not contemplated by the FCRA.**

The Proposed Rule purports to codify a definition of "consumer report" that is overbroad and will have significant negative consequences. The overbreadth is a result of the definition covering any expectation of how information may be used, in proposed section 1022.4(a)(2), and covering communications if they are used by a downstream recipient for a relevant purpose, even if the provider did not intend such use, as reflected in proposed section 1022.4(b). With these broad definitions, the safe harbor for companies that have no reasonable expectation that the information will be used for a relevant, credit-related purpose (see proposed section 1022.4(c)), is effectively useless to organizations – including companies that may be considered "data brokers" – that attempt to comply in good faith.

Taken together, the "consumer report" definition means that an entity will be considered a "credit reporting agency" as long as any recipient of information uses it for one of those specified purposes. If so, the communication of the information would constitute a consumer report (assuming the other elements of that definition are met), regardless of whether the person communicating the information collected the information or expected the information to be used for a credit-related purpose.[3] Furthermore, the Proposed Rule also extends to any entity if any downstream recipient of information — not just the immediate recipient of the communication — used the information for a specified purpose.[4]

This runs afoul of the FCRA. Contrary to proposed section 1022.4(b), under which a "consumer report" may exist regardless of an entity's knowledge or intent, it is well established that reports used or intended to be used for commercial purposes do not qualify as permissible purposes under the FCRA.[5] This is because the FCRA plainly states that "consumer reports" must be used or expected to be used for the purposes the FCRA specifies.[6]

Notably, in the NPRM, the CFPB also identifies national security harms from the disclosure of personal information of military service members and government employees to foreign adversaries that use the information for coercion, blackmail, and espionage.[7] While we take national security seriously, the FCRA is not a national security statute. The Proposed Rule's sweeping restrictions on the use of certain consumer data for domestic purposes lack any logical nexus to or justification on national security grounds. Rather, national security concerns should be addressed through existing laws and regulations focused on those issues, such as export control laws or through the enactment of the Protecting Americans' Data from Foreign Adversaries Act of 2024 (the "Act"). The Act, which enters into force on June 24, 2024, prohibits

[3] *See Id.*

[4] *See Id.*

[5] *See Ippolito v. WNS, Inc.*, 864 F.2d 440 (1988).

[6] *See* 15 USC 1681(d)(1).

[7] *See* 89 Fed. Reg. at 101405 and 101411-12.

a "data broker" from sharing and selling personally identifiable sensitive data of a U.S. individual to entities connected to China, Iran, North Korea, and Russia. These new legal prohibitions follow President Biden's February 2024 Executive Order and the corresponding U.S. Department of Justice (DOJ) Advance Notice of Proposed Rulemaking, which restrict the sale of sensitive data to countries of concern.

2. **The sweep of the 1022.4(a)(2) language would cover many publishers that routinely sell information to third parties that, while they could potentially be used for a permissible purpose, are intended for completely different purposes than those contemplated by the FCRA.**

As written, the definition of "consumer report" sweeps in (among other things) social media platforms, professional directories, databases of newspaper articles and other public domain material. In essence, it risks covering almost any entity that sells or shares information that *could* be used for a credit-related purpose.

We are concerned that this broad definition would curtail important, economically productive uses of data that are essential to the modern economy. Many data analytics companies that would be captured under the definition are involved in conducting analyses on publicly-available or commercially-available data, including even de-identified data, for societally beneficial ends such as identity verification, fraud detection and prevention, locating missing persons and persons entitled to government benefits, and law enforcement, or for commercial purposes such as product development, personalization of products and services, advertising, model development, and business-to-business intelligence. The compilation of data for these purposes falls outside the scope of the FCRA's definition of consumer reports, yet would be captured by this Proposed Rule.

In fact, the breadth of this definition could easily cover transactions as attenuated from consumer reporting as those between data brokers and online advertisers that are using digital platforms to reach consumers. Brokers and digital platforms frequently furnish these advertisers with data designed to aid in reaching those likely to be interested in the product being advertised – including data that could feasibly bear on creditworthiness and employment. Grocery stores, big box retailers, and pharmacies target advertisements to lower income consumers to inform them of government benefits, including the Supplemental Nutritional Assistance Program, Women, Infants, and Children (WIC), Medicaid, and related discounts. The Proposed Rule's restrictions on using data for targeted advertising would also limit the ability of government agencies, non-profit organizations, and advocacy groups to provide targeted information to consumers in low-income communities about benefits or services available to them.

Targeted advertising also avoids businesses bombarding consumers with advertising for products and services that are unlikely to interest them. Yet the Proposed Rule would prevent businesses from targeting products, services, or discounts tailored to individuals in, for example, income brackets that are most likely to have an interest in them. This is because if this

information were ever used for a permissible purpose under the FCRA, the Proposed Rule would cover the "data broker," and arguably the digital platform, as a "consumer reporting agency," even though it is simply being used to place relevant ads rather than make active determinations about employment or credit. In this way, the Proposed Rule would restrict 1) product development and enhancement efforts, 2) the ability of businesses to use consumer data obtained from data sources to personalize their products or services for consumers, and 3) even the use of a consumer's income or financial tier for AI benchmarking to ensure fairness, prevent discrimination, and ensure model output accuracy.

3. **The 1022.4(b) definition of "consumer report" would chill protected speech and interfere with productive business activity and fraud prevention because it applies to any downstream recipient, regardless of whether the entity communicating information intends this data to be used for credit decisions, employment purposes, insurance decisions, or other permissible purposes.**

The prong of the "consumer report" analysis that considers whether any recipient of the information used the information for one of the specified purposes – not just the immediate recipient of the communication – would create dramatic ramifications for the entire information economy and is unsupported by case law, regulatory interpretation, or congressional intent. Due to the vagueness and uncertainty of how downstream third parties would use this information, it also risks running afoul of the First Amendment by restricting the dissemination of large swaths of data, including even publicly available information, were this data to ever be used for a permissible purpose downstream and outside of a broker's control, despite its provenance and intent. This uncertainty would not only chill protected speech, but interfere with uses of data that protect consumers from crimes such as identity theft, and with other productive business activity, chilling business transactions and creating enormous compliance costs that will render critical data-driven services increasingly or even impossibly costly.

Specifically, the Proposed Rule would treat the downstream sharing of any information about a consumer's credit history, credit score, debt payments, or income or financial tier for any purpose as a consumer report. It would do so regardless of the actual reasons for previously collecting, sharing, or using the data. Put another way, information about a consumer's credit history, credit score, debt payments, or income could be obtained and used only and ever for FCRA permissible purposes. These include extending credit or insurance to consumers for personal, family, or household purposes, employment purposes, opening a bank account, or renting an apartment.

Uses such as research, modeling, marketing, law enforcement, small business transactions, and online fraud or retail fraud prevention would be prohibited under the Proposed Rule, and companies providing any of these data categories to third parties would then be treated as consumer reporting agencies. In practice, the Proposed Rule therefore would prohibit use of these types of data for many legitimate and beneficial commercial activities – including product development, personalization, advertising, and AI model benchmarking. None

of these activities are "permissible purposes" under the FCRA, so a person could not obtain such data from a third party to use for these activities.

In addition, were this rule implemented, even contractual obligations that flow down with this data — which themselves significantly increase compliance costs and potential oversight challenges — would be insufficient to protect "data brokers" from the potential for coverage under the FCRA. The Proposed Rule grants no immunity for data brokers who implement contractual or even oversight controls over the use of the information if a third party uses it for a permissible purpose, including in breach of this contract. Thus, a "data broker" would remain wholly exposed to the behavior and data use of the recipient. It is impossible to imagine that such a severe standard would not dramatically reduce information transfers out of well-intentioned compliance concerns alone.

For example, credit header data is obtained and used for identity verification and fraud detection purposes. Some of those contexts involve FCRA permissible purposes, including verifying a consumer's identity or detecting and preventing potential fraud in connection with a credit transaction, employment, or requests for government benefits. Yet defining credit header data as a consumer report would harm fraud prevention efforts by forcing a wholesale remap of these prevention systems. Searching consumer reports for the purposes of fraud prevention involves a 1:1 search for a variety of connections, including, for example, the frequency of a social security number's use, or personally identifying information being used as part of the creation of synthetic identities. Covering this under the Proposed Rule would harm financial services fraud prevention platforms and in turn their consumers, and even future customer applicants.

Furthermore, credit header data is also used for these purposes in other contexts that do *not* involve FCRA permissible purposes. For example, credit header information might be used to prevent retail fraud by matching billing address on account against credit header data for a cardholder, detect fake reviews where listed address does not match credit header data, or verify age of users to prevent child access to inappropriate content. Under the Proposed Rule, however, a third party would be unable to purchase credit header data to include in its identity verification tool or its fraud detection or prevention tool, *unless* it provides that tool only to end users who have a permissible purpose under the FCRA. The third party would then also be deemed a consumer reporting agency that is furnishing consumer reports under the Proposed Rule, even if it does not provide the credit header data to its end user customers – simply because it facilitates the merchant's use of the credit header data for the merchant's financial gain. This would deal a severe blow to the entire information economy.

* * *

Thank you for considering our views. We look forward to continued engagement with the Bureau and would be happy to discuss any of these issues further with you.

Respectfully submitted,

Anton van Seventer
Counsel, Privacy & Data Policy
Software & Information Industry Association