Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

CDIAONLINE.ORG

July 14, 2023

Via Electronic Delivery to
DataBrokersRFI_2023@cfpb.gov

Consumer Financial Protection Bureau
c/o Legal Division Docket Manager
1700 G Street, NW
Washington, DC 20552

RE: Request for Information Regarding Data Brokers and Other Business Practices

To Whom It May Concern:

The Consumer Data Industry Association (CDIA) submits this comment letter in response to the request for information related to data brokers from the Consumer Financial Protection Bureau (CFPB).

CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies (CRAs), including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members provide a range of consumer data services that benefit not just end users, but consumers and the public at large. Outside of consumer report products governed by the Fair Credit Reporting Act (FCRA), these data services are extensively and effectively regulated by federal law and regulators. The FCRA does not regulate "data brokers" as the term is typically used, and there is no need for it to do so.

I. Access to Consumer Information Benefits Consumers and the Public at Large.

CDIA members enable businesses, governments, and volunteer organizations to access information on consumers for a range of uses. Those uses include consumer reports governed

by the FCRA, which are created when CRAs assemble or evaluate consumer information and which are provided for users to make eligibility decisions, like approving and denying consumer credit applications. The FCRA does not, however, govern data *intermediaries* that simply act as a conduit or pass-through of data from one party to another without "assembling or evaluating" the data.[1] Additionally, the FCRA does not govern data when it is provided for uses other than eligibility decisions. Non-eligibility uses are incredibly important to consumers and the public at large, though, and CDIA members provide for these uses by complying with existing law and consumer expectation.

Within this current regulatory framework, benefits fostered outside of FCRA-governed eligibility uses include the following:

Identity Verification and Authentication: In an increasingly mobile society, consumer data applications are integral to authenticating the right person, location, and device. Identity verification and authentication solutions return to users indicia of fraud or other improper activity. These products are not used solely to deny applications, so these uses are not *eligibility* uses. They rely on data like credit header data that are governed by laws other than the FCRA, namely the Gramm-Leach-Bliley Act (GLBA). For example, online authentication plays a key role in customer convenience in online transactions, where consumers can use their trusted online identities to complete transactions on their timelines through the use of third-party data. At the airport, trusted identity programs driven by consumer data speed travelers through security while enhancing public safety. Identity verification and authentication solutions reduce friction in person and online to make transactions more seamless.

Consumer Fraud Prevention: Consumer data and analytics solutions enhance protection against identity theft while meeting consumers' convenience expectations outside of identity verification and authentication applications. The FTC recognized the benefit that data has in fraud prevention in its report on Big Data.[2] Fraud prevention and detection services provide information on known fraudsters and fraud strategies and identify potential fraud risks based on comparing applicant-supplied data with data available from third-party sources as well as historic transactions and observed behaviors. Subscribers of these types of services use the information provided to mitigate fraud losses. The savings realized by the subscribers result in lower-cost products and services, ultimately benefiting consumers. Consumers are also able to access monitoring products directly to be alerted to identity or fraud issues that may impact them. For example, fraudulent tenant and mortgage applications, as well as fake landlord offers and mortgage swindles, are reduced by consumer data and

---

[1] 12 U.S.C. § 1681a(f).

[2] FTC, *Big Data: A Tool for Inclusion or Exclusion*, at 5 ("[M]ining large data sets to find useful, non-obvious patters is a relatively new but growing practice in… fraud prevention."), Jan. 2006, *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

analytics providers' fraud prevention and verification tools. Fast consumer lending fraud prevention relies on a consumer data network supported by a sophisticated system of consumer data aggregators, analysts, and application providers. Even fraud in consumer disputes from credit repair organizations—which the CFPB has rightly targeted—is reduced with anti-fraud verification from consumer data and analytics providers.

Commercial and Government Fraud Prevention: Federal, state, and local government benefits programs also depend significantly on CDIA-member consumer data and analytics providers to root out applicant fraud. Consumer data and analytics providers help limit fraud in SNAP benefit awards[3] and tax refunds.[4] Health care plans and regulators rely on CDIA-member consumer data and analytics providers to identify health care provider program fraud.[5] New consumer data collection and analytics are often correctly suggested as a key solution to fraud. Two 2023 examples: Addressing the COVID-era spike in improper federal benefits payments, the Government Accountability Office (GAO) earlier this year recommended establishing wider use of consumer data analytics services and wider consumer data sharing, specifically "a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud" and making "permanent the requirement for the Social Security Administration to share its full death data with Treasury's Do Not Pay working system."[6] Addressing concerns over fraud in the Immigrant Investor Program (EB-5 visa), the GAO called for additional data collection and "additional screening of investors from countries of concern."[7]

Law Enforcement Investigation: Federal, state, and local law enforcement depend on consumer data and analytics providers for a wide range of staffing and investigative tools, including crime mapping and lead investigation.[8]

Insurance Beneficiary Location: Insurance providers, particularly life insurance providers, depend on consumer data companies to identify and locate beneficiaries who may have moved since their address was last provided.

Risk Management: Corporate and public safety are promoted through the sharing of experiential learning and public consumer data among data and analytics providers. Commercial driver safety, consumer insurance, contract (including credit) default risk, and

---

3 *See* https://risk.lexisnexis.com/insights-resources/research/true-cost-of-fraud-study-for-snap.

4 *See* https://www.irs.gov/newsroom/new-identity-verification-process-to-access-certain-irs-online-tools-and-services.

5 *See* https://risk.lexisnexis.com/insights-resources/case-study/healthcare-billing-and-fraud-detection.

6 "Emergency Relief Funds: Significant Improvements are Needed to Address Fraud and Improper Payments," U.S. Govt. Acct. Ofc., GAO-23-106556, Feb. 1, 2023, https://www.gao.gov/products/gao-23-106556.

7 *See* https://www.gao.gov/assets/gao-23-106452-highlights.pdf.

8 *See* https://risk.lexisnexis.com/law-enforcement-and-public-safety.

crime risk are managed more effectively by the aggregation, analysis, and prompt delivery of accurate consumer data to user decision processes.

Discrimination Prevention: Consumer data is aggregated and normalized for the purpose of evaluating compliance by credit providers with fair lending and community reinvestment laws.

Public Interest Research: Unique national, local, and industry behavioral trends information is available from consumer data and analytics providers for providing important public benefits. Social media intelligence helps better understand and address loneliness among users, a current priority public health concern.[9] COVID-era analyses from consumer data providers helps policymakers better understand the impact of the pandemic on consumer credit, health, residency movement, and other key aspects of life. Consumer data aggregators aggregate and deliver unique data sets for university and non-profit research. Research into court system activity, for example, is made possible and enhanced by court data unavailable from the courts but provided uniquely by CDIA members.

II. The FCRA and the Dodd-Frank Act Do Not Permit the CFPB to Regulate Data Brokers under the FCRA.

The CFPB does not make entirely clear whether the RFI is intended to aid potential rulemaking or informal agency pronouncements, nor does it make clear how the RFI might provide insight into topics that it might have authority to regulate. The agency does hint, concerningly, that the RFI is in part intended to inform its "planned rulemaking under the FCRA."[10] What is clear is that neither the FCRA nor the Dodd-Frank Act permit the CFPB to regulate non-CRA data brokers under the FCRA.

The FCRA permits the CFPB to "prescribe regulations as may be necessary or appropriate to administer and carry out the purposes and objectives of" the FCRA, which shall apply "to any person that is subject to the FCRA." *See* 15 U.S.C. § 1681s(e). This means that the Bureau's authority is limited to regulations that are "necessary or appropriate" to carry out the objectives of the FCRA, but only to the extent that it regulates the conduct of those persons subject to the FCRA, namely, consumer reporting agencies, furnishers, users, and consumers. A person is only a consumer reporting agency if that person meets the multi-faceted definition of consumer reporting agency and that person is selling a "consumer report," as defined. A

---

[9] Surgeon General Murthy has made the epidemic of loneliness and isolation the subject of his most recent Surgeon General Advisory. *See* https://www.hhs.gov/about/news/2023/05/03/new-surgeon-general-advisory-raises-alarm-about-devastating-impact-epidemic-loneliness-isolation-united-states.html.

[10] *See* CFPB, *Press Release: CFPB Launches Inquiry Into the Business Practices of Data Brokers* (Mar. 15, 2023), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/.

consumer reporting agency is a person who, "for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f). Not all data or communications about consumers meet the definition of "consumer report"; a "consumer report" means:

> "any written, oral, or other communication of any 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 which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [§ 1681b]."

15 U.S.C. § 1681a(d). Thus, the person engaging in the activity must be: (i) assembling or evaluating (ii) information on consumers (iii) for the purpose of furnishing consumer reports (iv) to third parties (v) using interstate commerce to prepare or furnish such reports. Further, the information being communicated to a third party must be for an FCRA purpose—namely, eligibility for consumer credit, employment, and other purposes only permitted by §1681b(a) of the FCRA—and must be "used or expected to be used" for an FCRA permissible purpose. If any one of these elements is not met, the FCRA does not apply.

The CFPB takes the position that "data brokers," "data aggregators," and "platforms" "all share fundamental characteristics with consumer reporting agencies – they collect and sell personal data." RFI, p. 4. The CFPB's position contradicts the comprehensive definitions enacted by Congress as interpreted by the FTC and other federal regulators for decades. Neither the rulemaking provision of the FCRA nor those of the Dodd-Frank Act permit the CFPB to change the scope of 'persons' subject to the FCRA. Nor do these rulemaking provisions—or any part of Dodd-Frank—authorize the CFPB to utilize its UDAAP authority to modify the FCRA's express definitions or scope or otherwise incorporate data brokers into its authority.

Under Dodd-Frank, the CFPB's rulemaking authority extends only to the regulation of consumer financial products and services, as defined by that law. Many of the data products discussed above are not "financial products or services" under that definition.[11] Therefore, the CFPB does not have authority over those product offerings. Further, the CFPB's rulemaking powers—including under UDAAP prohibitions—expressly exclude certain consumer reporting

[11] *See* 12 U.S.C. § 5481(15)(A).

activities, such as the provision of information for purposes of employment or tenancy decisions and for products and services for fraud or identity theft detection, prevention, or investigation.[12]

There is no uncertainty around the scope of the FCRA, particularly whether some defined set of "data brokers" are CRAs.[13] In its 2012 report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Consumers* ("Privacy Report"),[14] the FTC delineated three categories of data brokers: (1) entities that maintain data for marketing purposes; (2) non-FCRA covered entities that maintain data for nonmarketing purposes that fall outside of the FCRA, such as to detect fraud or locate people; and (3) entities that are subject to the FCRA.[15] The test for whether a data broker falls within the third category has been long understood, and is straightforward: "to the extent that they are providing 'consumer reports'," data brokers are CRAs and thus subject to the requirements of the FCRA.[16]

For years, the FTC has consistently applied this test and used its enforcement authority under the FCRA to take action against companies operating within the FCRA's ambit. Recent examples abound. In 2020, the FTC took action against CRA AppFolio relating to consumer information sourced from a third-party data vendor, which the FTC acknowledged was not a CRA where it disclaimed any guarantee relating to accuracy and

---

[12] *Id.* at 5481(15)(A)(ix)(I)(cc) and 5481(B)(i)(II).

[13] Moreover, if a CFPB advisory opinion were to go beyond addressing some uncertainty, such as clarifying the meaning of ambiguous terms in the law, by imposing specific requirements or a new standard of law on data brokers, it would risk being judicially deemed invalid. To impose new legal requirements or standards the agency must proceed with APA rulemaking, including notice and comment. *See, e.g.*, *United States v. Picciotto*, 875 F.2d 345, 347 (D.C. Cir. 1989); *Am. Hospital Assoc. v. Bowen*, 834 F.2d 1037, 1044-45 (D.C. Cir. 1987); *Guedes v. Bureau of Alcohol, Tobacco, Firearms & Explosives*, 920 F.3d 1, 29 (D.C. Cir.), *judgment entered*, 762 F. App'x 7 (D.C. Cir. 2019). But, as noted earlier, whether the CFPB can even engage in rulemaking in connection with relevant subject matter is questionable.

[14] *Available a*t https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[15] *See also* Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability, at i (May 2014) (reiterating the three categories data brokers identified in the Privacy Report), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[16] *See, e.g.,* Prepared Statement of the Fed. Trade Comm'n, Before the Subcomm. on Fin. Inst. and Consumer Credit Comm. on Fin. Servs. U.S. House of Representatives on Enhancing Data Security: The Regulators' Perspective, at 8 (May 18, 2005), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-subcommittee-financial-institutions-and-consumer-credit/050518databrokertestimonyparnes.pdf.

required AppFolio to verify the information.[17] In 2021, the agency issued warning letters to several mobile app developers that compiled public record information to create background and criminal record reports, cautioning that companies who provide information to, say, employers regarding employees' criminal histories, are providing "consumer reports" because the data involves the individual's character, reputation, or personal characteristics, and such companies must therefore comply with the FCRA.[18] That same year, the FTC settled allegations against Spokeo, Inc., a company that collected personal information about individuals from hundreds of online and offline data sources and merged the data to create detailed personal profiles of consumers, which was then marketed on a subscription basis to job recruiters and others as an employment screening tool. The FTC determined that that collection of information constituted a consumer report and that Spokeo was a CRA subject to the FCRA.[19] The FTC also settled with two other data brokers who allegedly sold "consumer reports," compiled using public record information, to employers and landlords without taking reasonable steps to make sure that they were accurate as required by the FCRA.[20] The FTC has enforced the FCRA against entities only where it alleges the entity is a CRA, and it has done so consistently. FCRA enforcement history demonstrates no uncertainty around the scope and applicability of the FCRA.

Furthermore, the CFPB does not have authority to regulate non-CRA data brokers under the FCRA by way of the Advisory Opinion Policy. The CFPB's Advisory Opinion Policy, which, in short, sets out agency procedures for interested parties to submit requests that the CFPB issue advisory opinions, allows the CFPB to issue such interpretive rules to *clarify* but not *rewrite* the law.[21]

Finally, not only would the CFPB be without authority to regulate data companies that are not CRAs under the FCRA, but it would be unfair to attempt to do so. Companies operating within and outside of the FCRA have taken note and relied on the plain language

---

[17] Fed. Trade Comm'n v. AppFolio, Inc., *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/1923016-appfolio-inc.

[18] Fed. Trade Comm'n, *Press Release: FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act* (Feb. 7, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting-act.

[19] *United States v. Spokeo, Inc.*, No. 2:12-cv-5001 (C.D. Cal. June 12, 2012), https://www.ftc.gov/legal-library/browse/cases-proceedings/1023163-spokeo-inc.

[20] Fed. Trade Comm'n, *Press Release: Two Data Brokers Settle FTC Charges That They Sold Consumer Data Without Complying With Protections Required Under the Fair Credit Reporting Act* (Apr. 9, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/04/two-data-brokers-settle-ftc-charges-they-sold-consumer-data-without-complying-protections-required.

[21] 85 Fed. Reg. 77987 (Dec. 3, 2020) ("The Bureau will focus primarily on clarifying ambiguities in its regulations, although Advisory Opinions may clarify statutory ambiguities. The Bureau will not issue advisory opinions on issues that require, or are better addressed through, a legislative rulemaking under the APA. For example, the Bureau does not intend to issue an advisory opinion that would change regulation text or commentary.").

and consistent regulatory enforcement and guidance history to build compliance structures, make business strategy decisions, and manage regulatory risk. It would be unfair and would undermine the Bureau's authority to attempt to make regulatory pronouncements or take enforcement actions that are contrary to industry's reasonable reliance on past agency actions.

III. Access to and Use of Consumer Information is Sufficiently Regulated.

Accessing and using consumer information is regulated by both state and federal law, by data source, data type, and data use. Setting aside state laws, federal laws that regulate consumer information not provided as consumer reports—like by data brokers—include the following:

GLBA: The Gramm-Leach-Bliley Act provides consumers with rights to understand financial institutions' privacy practices, rights to opt out of certain information sharing, and restricts third-party recipients' use and further disclosure of information from financial institutions to certain permitted purposes. CDIA members ensure that GLBA data are provided only for these purposes. Additionally, the Safeguards Rule, promulgated under GLBA, requires financial institutions to implement and maintain certain controls to protect the security, integrity, and confidentiality of consumer data. Specifically, the Rule imposes standards prohibiting the unauthorized disclosure of customer information, requiring service providers to implement and maintain those same controls, and requiring the secure disposal of customer information.

DPPA: The Driver's Privacy Protection Act limits access to and use of information from state motor vehicle departments to certain lawful uses. Like with GLBA, CDIA members provide DPPA-regulated data only for permitted uses.

UDA(A)P: The FTC and the CFPB have the broad ability to prohibit acts and practices that are unfair, deceptive, or in the case of the CFPB, abusive toward consumers. CDIA members engage in UDAAP analyses when building or revising products to ensure that consumer information is handled consistent with consumer expectations.

COPPA: The Children's Online Privacy Protection Act (COPPA) meaningfully constrains the use of personal information about minors. The FTC, on its own and in collaboration with state attorneys general, has reached major settlements under existing rules with video game makers and video and technology providers over COPPA allegations.[22]

---

[22] Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges, Dec. 19, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations; Google and YouTube Will Pay Record $170 Million for Alleged Violations of

HIPAA: Since 2002, the Health Insurance Portability and Accountability Act (HIPAA) has imposed substantial data privacy and security obligations on covered holders of consumers' health information, known as protected health information (PHI). Substantial regulatory settlements are regularly obtained for alleged violations of HIPAA rules.[23]

Anti-discrimination laws: Federal law contains a range of anti-discrimination laws in various sectors, including the Equal Credit Opportunity Act (ECOA), the Fair Housing Act (FHA), and Title VII of the Civil Rights Act of 1964. These laws apply to the use of consumer information in these contexts, whether by end users or by entities that may use algorithms to create scores or other analyses.

Federal regulators have demonstrated the ability and willingness to hold data brokers accountable for harmful practices through these laws. For example, the FTC and DOJ took action against MyLife.com for allegedly deceiving consumers through "teaser background reports" that did not include criminal record information that the company advertised.[24] The FTC also took action against LeapLab for allegedly selling sensitive information including Social Security Numbers and bank account numbers to scammers.[25] Finally, the FTC took action against Sequoia One and related entities for allegedly collecting consumer information for payday loan consideration and sold it to third parties that initiated card transactions without the consumers' consent through its Section 5 UDAP authority.[26]

In the RFI, the CFPB identified four harms and abuses related to data brokers: (1) privacy and security risks; (2) the facilitation of fraud or abuse; (3) the lack of consumer knowledge and consent; and (4) the spread of inaccurate information. The laws discussed above address all of these issues and appropriately arm the Bureau or other agencies to prevent consumer harm or abuse. On privacy and security, federal laws impose standards appropriate to the nature of the data, likely under GLBA, DPPA, or HIPAA. Federal anti-discrimination laws are useful to prevent certain harmful behavior, as are UDAAP standards. UDAAP standards also are useful to address issues related to consumer knowledge and consent as well as inaccurate information. It is also worth noting that inaccurate information may be useful in fraud applications to return fraud indicia, all consistent with UDAAP prohibitions. The FCRA is not needed to address consumer harms or abuses by data brokers.

Children's Privacy Law, Sept. 4, 2019, https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.

[23] Anthem pays OCR $16 Million in record HIPAA settlement following largest health data breach in history, Oct. 15, 2018, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html.

[24] Fed. Trade Comm'n v. MyLife.com, Inc., et al., *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3022-mylifecom-inc.

[25] Fed. Trade Comm'n v. Sitesearch Corp. d/b/a LeapLab, *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/142-3192-x150060-sitesearch-corporation-doing-business-leaplab.

[26] Fed. Trade Comm'n v. Sequoia One, LLC, et al., *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3253-x150055-sequoia-one-llc.

The FCRA is needed to address consumer harms and abuses by CRAs. When passing and amending the FCRA, Congress made the determination that *for certain kinds of uses*, entities providing consumer information must extend additional rights to consumers and comply with obligations beyond those in the laws listed above. The FCRA applies to consumer information provided for eligibility purposes; that is, where the information is provided and used to make a decision as to whether the consumer is eligible for credit, insurance, employment, housing, or certain other benefits. Special protections under the FCRA include limiting the purposes for which information may be shared, requiring that data users must be verified, limiting the information that may be provided for eligibility purposes, and extending consumers' rights (including rights to access, dispute, and opt out of prescreening).

These special protections do not apply to an intermediary that stands merely as a conduit between a data source and a data user. Thus, the FCRA, by its plain language (as well as a history of cases and regulatory interpretations), applies where those entities *assemble or evaluate* the information to provide them in reports *to third parties*. 15 U.S.C. § 1681a(f). The FCRA does not apply to these data intermediaries even where those intermediaries permit data users to make eligibility decisions based on the information, where those intermediaries play a limited role in sourcing and processing the information. Congress struck a policy balance in defining CRAs subject to the FCRA by considering not only the need to protect consumer privacy but also the benefits to consumers and the economy from the use of such data. Attempting to regulate data brokers that are not CRAs like they were CRAs would disrupt this balance and would not be consistent with that clearly-expressed intent to ensure that entities employ reasonable procedures to use consumer data fairly and equitably when evaluating a consumer's eligibility for consumer credit, employment, insurance, or certain other purposes.[27]

Similarly, it would be inconsistent with Congress' clearly expressed intent to regulate non-CRA data brokers as CRAs where they do not provide consumer information for eligibility purposes, but instead for purposes discussed above, like verifying identity and detecting fraud. Consumer informion here includes credit header information, which is regulated by the laws discussed above. There are strong policy reasons for such restraint. Imposing FCRA regulations in this context would have a devastating impact on users who rely on these services without meaningful benefit to consumers. That impact would be felt far and wide. For example, certain anti-fraud products function by collecting device data about a consumer's personal device and sharing that information with third-parties who analyze that data *and* combine it with data from other sources related to that device to flag indicators that a transaction may pose a fraud risk. Because products are built on complex data interplays, limiting data available for fraud prevention—by applying FCRA rules—would affect not only the consumer whose data is removed, but all individuals.

---

[27] 15 U.S.C. § 1681.

Finally, it would also broadly be inappropriate to subject non-FCRA activities to regulation not designed for such activities. As an example, the FCRA's permissible purpose framework may not even permit certain uses without consumer consent, which would undermine the effectiveness of a service like fraud detection. Extending access rights to data held for fraud detection purposes would permit fraudsters to steal public benefits. Permitting fraudsters to use FCRA dispute channels would present new opportunities to steal consumer identities. The FCRA's protections are not fit for non-eligibility uses that are essential to protecting consumers and maintaining the public welfare.

For all the foregoing reasons, CDIA urges the CFPB to recognize the tools available and useful for preventing consumer harm by data brokers and, for the FCRA, to defend Congressional intent, the plain language of the law, and the history of regulatory interpretation.

* * *

We appreciate the opportunity to comment on the CFPB's RFI and hope the Bureau will find these comments useful.

Sincerely,

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs