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

November 6, 2023

Via Electronic Delivery to
CFPB_consumerreporting_rulemaking@cfpb.gov

Consumer Financial Protection Bureau
c/o Comment Intake Request
1700 G Street, NW
Washington, DC 20552

RE: Small Business Advisory Review Panel for Consumer Reporting Rulemaking – Outline of Proposals and Alternatives Under Consideration

To Whom It May Concern:

The Consumer Data Industry Association (CDIA) submits this comment letter in response to the Small Business Advisory Review Panel for Consumer Reporting Rulemaking – Outline of Proposals and Alternatives Under Consideration (Outline) 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.

Through the proposals reflected in the Outline, the CFPB has indicated its consideration of regulations under the Fair Credit Reporting Act (FCRA) that will have far-reaching, and industry-altering effects, many of which will have significant negative impacts on small businesses, on consumers, and on the consumer reporting industry as a whole. The nation's consumer reporting system is too important to the economy to proceed without an adequate understanding of the consequences, both intended and unintended, of the proposals under consideration. As CFPB Director Richard Cordray observed:

> Credit reporting is an important element in promoting access to credit that a consumer can afford to repay. Without credit reporting, consumers would not be

> able to get credit except from those who have already had direct experience with them, for example from local merchants who know whether or not they regularly pay their bills. This was the case fifty or a hundred years ago with "store credit," or when consumers really only had the option of going to their local bank. But now, consumers can instantly access credit because lenders everywhere can look to credit scores to provide a uniform benchmark for assessing risk. Conversely, credit reporting may also help reinforce consumer incentives to avoid falling behind on payments, or not paying back loans at all. After all, many consumers are aware that they should make efforts to build solid credit.[1]

Given the potential impacts of the proposals, CDIA submits the following comments, but given the fact that the Outline only addresses proposals that are likely to have a material impact on small business entities, we encourage the CFPB to obtain broad stakeholder input on all FCRA rulemaking proposals and others, through an advanced notice of proposed rulemaking, stakeholder meetings, and/or other open forums.

I. The SBREFA Outline Lacks the Specificity Needed to Permit Small Businesses to Comment Meaningfully on the Proposals.

In many material parts, the lack of clarity and specificity in the Outline compromises the spirit and requirements set forth in the Small Business Regulatory Enforcement Fairness Act (SBREFA). For example, it is difficult to provide meaningful feedback on dispute rule proposals when the CFPB has not expressed concrete concerns related to what the CFPB considers a "systemic" issue, other than that it is an issue that affects multiple consumers. Similarly, it is difficult, if not impossible, to estimate required improvements and the associated costs that would be incurred if the CFPB were to issue a rule seeking to treat "all data breaches" as violations of the FCRA (essentially a strict liability standard) when "all data breaches" is not defined. We have addressed these and other areas in our comments below, but note that the overarching lack of specificity and clarity in the Outline does not meet the purpose or spirit of the SBREFA process, which is to obtain input from small businesses that are likely to be directly affected by the regulations that the agency may issue.

II. The CFPB's Rulemaking Authority Does Not Allow It to Rewrite the Statute or Insert Wholly New Requirements.

"It is axiomatic that an administrative agency's power to promulgate legislative regulations is limited to the authority delegated by Congress."[2] Here, Congress delegated to the CFPB *limited* rulemaking authority with regard to the FCRA – to "prescribe regulations as may be necessary or appropriate to administer and carry out the purposes and objectives of [the FCRA], and to prevent evasions thereof or to facilitate compliance therewith", which shall

---

[1] https://www.consumerfinance.gov/about-us/events/archive-past-events/field-hearing-on-new-credit-reporting-supervision-detroit-michigan/

[2] *Bowen v. Georgetown Univ. Hosp.,* 488 U.S. 204, 208 (1988).

apply "to any person that is subject to the FCRA."[3] This means that the CFPB's authority is limited to regulations that are "necessary or appropriate" to carry out the objectives of the FCRA with respect to persons deemed subject to the FCRA. This grant of authority does not permit the CFPB to create new obligations or change the language of the FCRA by establishing new requirements that ignore the language and purpose, or otherwise extending the scope of, the FCRA. Many of the proposals in the Outline suggest that the CFPB intends to do just that.

For example, the CFPB's proposal to transform data brokers into CRAs by recognizing that certain kinds of information are "typically used" in connection with an eligibility determination that falls within one of the FCRA's permissible purposes would not **carry out** the purpose of the FCRA – **it would change it**. Effectively, what the CFPB proposes to do is to redline the definition of consumer report to fundamentally change who is covered. The definition would label information as consumer report information that is of a nature commonly used, even if not actually "used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility" for a permissible purpose. This, the CFPB may not do.

"A decision of such magnitude and consequence" on a matter of "'earnest and profound debate across the country' must "res[t] with Congress itself, or an agency acting pursuant to a clear delegation from that representative body."[4] An agency's action will be held unreasonable where

> . . . it would bring about an enormous and transformative expansion in [the agency's] regulatory authority without clear congressional authorization. **When an agency claims to discover in a long-extant statute an unheralded power to regulate "a significant portion of the American economy," we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast "economic and political significance**."[5]

This rulemaking looks to be the same type of administrative overreach resulting in "an enormous and transformative expansion of the [CFPB's] authority without clear congressional authorization."[6]

---

[3] 15 U.S.C. § 1681s(e).
[4] *Biden v. Nebraska*, 143 S. Ct. 2355, 2374 (2023) (*quoting W. Virginia v. Env't Prot. Agency*, 142 S. Ct. 2587, 2615 (2022)).
[5] *Util. Air Reg. Group v. EPA*, 573 U.S. 302, 324 (2014) (emphasis added) (citations omitted).
[6] *Id. See also Chamber of Commerce v. CFPB,* Opinion and Order, No. 6:22-cv-00381 (E.D. Tex. Sept. 8, 2023)., at 18 (finding that the CFPB exceeded its authority in its March 2022 update to its Supervision and Examination Manual because the conferral of authority to regulate unfair acts or practices was "not the sort of 'exceedingly clear language' that the major-questions doctrine demands before finding a conferral of agency authority to regulate discrimination across the financial-services industry").

The same is true for the proposals that seek to limit the use of consumer reports **only** for eligibility purposes (as the proposal related to the legitimate business need permissible purpose seeks to do). In fact, Congress expressly contemplated that users would need, and should have access to, consumer report information for non-eligibility purposes, including:

- in accordance with the written instructions of the consumer to whom it relates;
- intends to use the information, as a potential investor or services, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an *existing* credit obligation
- for child support enforcement purposes; and
- to the FDIC and NCUA acting as conservator or receiver. [7]

Congress also has expressly authorized uses of data outside of an FCRA permissible purpose, which are already well-regulated. For example, any number of laws help to ensure the privacy of certain data sets and various use cases contemplated by the CFPB, including the Gramm-Leach Bliley Act; the Drivers Privacy Protection Act; the Childrens' Online Privacy Protection Act, the Health Insurance Portability and Accountability Act, and the federal anti-discrimination laws (such as the Equal Credit Opportunity Act). Under the proposed American Data Protection Privacy Act (ADPPA), Congress is considering a sweeping data privacy law that would govern access to and use of consumer data on a nationwide basis.[8] To the extent that the CFPB seeks to exercise its FCRA rulemaking authority to fill perceived gaps in the law (such as its expressed desire to address the activities of "data brokers"), CDIA asserts that such gaps are left to Congress, and are not a proper exercise of the CFPB's prescribed rulemaking authority under the FCRA.

III. The CFPB Should Finalize the Rulemaking on Personal Financial Data Rights and Ensure Broad Stakeholder Input Before Issuing a Proposed FCRA Rule.

Providers of consumer-permissioned data—like aggregators that may be impacted by the CFPB's Personal Financial Data Rights (PFDR) rulemaking—could also be impacted. Even acting within the consumer's permission, aggregators that currently are not CRAs may find themselves declared CRAs by CFPB rule. The PFDR Notice of Proposed Rulemaking notes that aggregators that meet the definition of a CRA under the FCRA would be subject to the FCRA in addition to the finalized rules. CDIA therefore encourages the CFPB to work to finalize the PFDR Rule before proposing any FCRA rule. Shifts in scope of the FCRA under an FCRA rulemaking could have major impacts on the workability of a PFDR Rule.

Because any proposal here has the potential to alter the consumer reporting ecosystem significantly, and have significant impact on entities of all sizes (small to large), CDIA requests

[7] 15 U.S.C. § 1681b(a)(2), § 1681b(a)(3)(E), § 1681b(a)(5), and § 1681b(a)(5).
[8] https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-HB512E26C49274B20A17C81D17DE0892E

that the CFPB ensure that it has full stakeholder involvement on the development of any rule in this area, such as through broader stakeholder meetings or by seeking input on more specific proposals through an advance notice of proposed rulemaking. By drawing bright line rules, the CFPB runs the risk of redefining the scope of the law rather than clarifying it. The CFPB might consider working with stakeholders to, for example, map out safe harbors for important non-FCRA information sharing such as technology platforms, consumer-permissioned data aggregators, sales agent relationships, or other conduits.

IV. Specific Proposals Under Consideration

A. Definitions of consumer report and consumer reporting agency.

1. Data brokers

In its Outline, the CFPB identifies several possible proposals by which it would attempt to regulate data brokers under the FCRA. These proposals ignore the reality that the data is neutral as to a particular consumer; it is only through the furnishing of the information by a CRA to an end user for a permissible purpose does it become a consumer report, to which FCRA obligations attach.

One proposal would provide that data brokers that sell certain categories of data would be CRAs under the FCRA, regardless of its intended use. Another proposal states that consumer information provided to a user (ostensibly, even for a non-FCRA purpose) that uses it for an FCRA permissible purpose should be a consumer report under the FCRA even when the user has violated the terms of restrictions prohibiting it from doing so. Of the several proposals in the Outline related to data brokers, these are most concerning to CDIA. Both proposals are inconsistent with the plain language of the FCRA, exceed the CFPB's statutory authority, would assign liability to blameless parties, and would negatively impact consumers and the public at large without countervailing benefits.

The Outline states that the term "data broker" is an umbrella term, encompassing any entity that collects, aggregates, sells, resells, licenses, or otherwise shares personal information about consumers with other parties, and that data brokers may or may not be CRAs. CDIA is troubled that the CFPB has invented this definition out of whole cloth for FCRA rulemaking purposes. CDIA is also troubled that the CFPB proposes to use this concept to expand the scope of the FCRA beyond Congress' clearly stated intent.

The first proposal—defining an entity as a CRA because it sells certain categories of data—overlooks elements of the definitions of CRA and consumer report under the FCRA, at least in the case of those certain data types. Beyond distinguishing consumer information that bears on one of the seven characteristics listed in the definition of "consumer report" and other information, the scope of the FCRA makes no distinction on data types; the FCRA cares about how data is actually used rather than assigning rules to specific information. Such a rule would ignore whether the entity "assembled or evaluated" the data, whether it provided the

data for an FCRA permissible purpose, whether the user is a third party, and other critical elements in these definitions. As a result, the market among data companies would contract, costs would rise, and entities collecting and selling certain data types would be unable to provide it for certain critical purposes outside the FCRA, such as to prevent or detect fraud or identity theft. Expansive privacy laws, like the various state consumer data privacy laws, are measured in their impact on large versus small businesses, but this proposal would damage data markets rather than protect them.

The second proposal—to treat certain information as a consumer report despite any contractual limitations and controls—is equally troubling. Even if a data company contractually prohibited users from using the information for an FCRA permissible purpose, and even if the data company has no reason to believe the user would violate its contract, this proposal would make such information a consumer report, meaning that data companies may be in the position of accidentally providing consumer reports. All data companies would then need to be prepared for the possibility that a customer may, by violation of contract, make the data company a CRA, subjecting it to regulation and statutory and private penalties. CRAs only have limited tools to prevent data misuse, including contracting. Further, audits, while helpful, can never fully prevent such misuse from occurring in the first instance. The result would be to raise the risks—and thus the costs—to data companies providing non-consumer report products, like fraud prevention products.

a. The CFPB has no authority to modify the definitions of the FCRA or expand the scope of the law.

As a threshold issue and as noted above, the CFPB does not have the authority to issue rules as the Outline describes them. The CFPB'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, CRAs, furnishers, users, and consumers.

Further, neither the FCRA rulemaking provisions, nor any part of Dodd-Frank, authorize the CFPB to use its UDAAP authority to modify the FCRA's express definitions or scope, or to 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 sought to be incorporated are not "financial products or services" under that definition.[9] 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 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.[10]

[9] *See* 12 U.S.C. § 5481(15)(A).
[10] *Id.* at 5481(15)(A)(ix)(I)(cc) and 5481(B)(i)(II).

The scope of the FCRA is well-established, , particularly whether some defined set of "data brokers" are CRAs. In its 2012 report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Consumers* ("Privacy Report"),[11] 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.[12] 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.[13]

b. Regulators have had no problem reining in data brokers they consider subject to the FCRA.

For years, the FTC has consistently applied the definition of "consumer reporting agency" and used its enforcement authority under the FCRA to take actions against companies operating within the FCRA's ambit. Recent examples abound. In 2020, the FTC took action against AppFolio (a CRA) 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 required AppFolio to verify the information.[14] 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, for example, 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.[15]

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

---

[11] *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.
[12] *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.
[13] *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.
[14] Fed. Trade Comm'n v. AppFolio, Inc., *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/1923016-appfolio-inc.
[15] 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.

screening tool. The FTC determined that that collection of information constituted a consumer report and that Spokeo was a CRA subject to the FCRA.[16] 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.[17] The FTC has enforced the FCRA against entities only where it alleges the entity is a CRA, and it has done so consistently.

c. The data broker proposals would harm consumers and the public at large.

These proposals would make it harder to provide fraud detection and prevention products. Because there is no "fraud prevention permissible purpose," users may be left with relying on written instructions to obtain such reports, which would be difficult—if not impossible—to obtain based on the ways fraud prevention tools are (and need to be) integrated into back-end processes, but would also undermine the purpose of the product itself. Additionally, imposing maximum possible accuracy procedure standards to data used in fraud detection and prevention products is not the appropriate standard for effective fraud prevention, where one needs to consider a broader swath of data to look for indicia of fraud. As a result, CDIA fully expects rates of identity theft and fraud to rise sharply.

Even when data may ultimately be provided in a consumer report, these data broker-related proposals may cause entities other than the CRA to become CRAs under the FCRA. Those include court researchers, wholesale public data companies, government database providers, and data aggregators. Many researchers, for example, are small businesses, and perform essential services like obtaining and verifying court records. The CFPB identifies criminal records as one type of record that collecting and sharing could make one a CRA. Thus, court researchers could be made CRAs, even when they merely provide data to CRAs for inclusion in consumer reports. The FCRA would already protect the ultimate use, and such treatment could create consumer confusion as to which entity the consumer should approach to exercise their rights under the FCRA. Imposing the same accuracy, dispute, and disclosure requirements on researchers as the CRAs would be untenable for many businesses unable to absorb the regulatory costs and risks. The proposal also does not seem to consider, let alone acknowledge, the impact on the courts, which are already resource-strained.

In addition to the two data broker-related proposals discussed above, the CFPB also proposes to prohibit companies that collect consumer information for an FCRA permissible purpose from selling such data for other purposes outside the FCRA. Court researchers similarly would be negatively impacted by this, as they often collect data for multiple clients at

---

[16] *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.

[17] 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.

once to maximize efficiency and lower costs. This proposal could prevent researchers from providing court data for fraud detection and prevention purposes if they initially pulled it for a background report

Finally, companies operating within and outside of the FCRA have relied on the plain language and consistent regulatory enforcement and guidance history to build compliance structures, make business strategy decisions, and manage regulatory risk. It would undermine the CFPB's authority to attempt to make regulatory pronouncements or take enforcement actions that are contrary to industry's reasonable reliance on past agency actions.

2. Defining "assembling or evaluating"

In the Outline, the CFPB acknowledges that there are entities that facilitate access to data when they act as intermediaries or vendors. The CFPB states that it is considering a proposal to provide a more bright-line definition for when such entities' activities fall within the meaning of the terms "assembling" and "evaluating" in the definition of "consumer reporting agency."[18] The CFPB's proposal, however, contains no details on what or where this bright line is, which prevents any meaningful comments or assessment by industry.

Courts that have addressed this issue have held that a CRA's business of assembling and evaluating consumer credit information involves "*more than receipt and retransmission*" of consumer financial information.[19] For example, in *Ori v. Fifth Third Bank,*[20] the court relied upon this distinction to conclude that claims against Fiserv, a company that provides technology solutions to financial services customers, should be dismissed because Fiserv is not a consumer reporting agency. Fiserv argued that:

> Fiserv is not a consumer reporting agency. It is a third-party data processor that financial institutions use to process transactions.... As part of the data processing services that Fiserv provides, it furnishes credit information to consumer reporting agencies. The information that Fiserv transmits to consumer reporting agencies consists of raw, unassembled data. The reporting agencies then use the data to construct, evaluate, and issue consumer credit reports... Fiserv, Inc. served as an outsourced-services vendor for Defendant Fifth Third Bank, and Fiserv, Inc. transmitted Fifth Third Bank's documents relating to current mortgages to major consumer reporting agencies...."[21]

The district court agreed that Fiserv was not a CRA and reasoned that "assemble" means to "bring together as in a particular place or for particular purpose." Based on that plain meaning, the court found that Fiserv did not assemble the information but instead merely transmitted information as a *conduit*. The court stated, "It is more reasonable to infer from plaintiff's

[18] Outline at 9-10.
[19] *See, e.g., McGrath v. Credit Lenders Service Agency, Inc.*, 2022 WL 580566 at *7 (E.D. Penn., Feb 25, 2022).
[20] 603 F. Supp. 2d 1171 (D. Wis. 2009).
[21] 2008 U.S. Dist. Ct. Motions 252986 (E.D. Wis. July 7, 2008).

allegations that Fiserv was a conduit which merely passed information about Fifth's mortgagors on to others. Obtaining and forwarding information does not make an entity a CRA."[22]

Furthermore, federal courts have concluded that entities were conduits and not CRAs when providing information from a variety of sources, including CRAs and government databases.[23] For example, the court in *Mix v. JP Morgan Chase Bank, NA* held in an order granting summary judgment for Chase Bank, that an entity, Fieldprint, which channeled fingerprints from Chase Bank to the Federal Bureau of Investigation (FBI) and subsequently, channeled criminal record history information from the FBI to Chase Bank, was not a CRA, but was rather a conduit of information.[24] The court reasoned that because Fieldprint passed "unadulterated information" to the FBI and to Chase,[25] Fieldprint was a conduit. Additionally, the court stated that Fieldprint did not "assemble or evaluate" information from the FBI or Chase by transmitting the data between the two.[26] According to the court, the relationship between Chase and Fieldprint and the FBI and Fieldprint was more akin to an agent/principal relationship rather than a CRA/end user relationship because Fieldprint was acting pursuant to a contract that did not specify that its actions would be governed through the FCRA, Chase was responsible for Fieldprint's compliance with FBI access terms, and Fieldprint had no control over Chase's employment decisions.[27]

---

[22] 603 F. Supp. 2d at 1175. *See Forty Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report and Summary of Interpretations* at 29 (providing that regarding "[c]onduit functions[,] [a]n entity that performs only mechanical tasks in connection with transmitting consumer information is not a [consumer reporting agency] because it does not assemble or evaluate information."); *see also Carlton v. ChoicePoint, Inc.*, No. 08-5779-RBK/KMW, 2009 U.S. Dist. LEXIS 109522, at *10-11, 15 (D.N.J. Nov. 23, 2009) (collecting cases for point that "assembling or evaluating" phrase "implies a function which involves more than receipt and retransmission of information," and dismissing claim because defendant was "merely a conduit of information, as opposed to an entity that in any way re-organizes or filters information" (citation omitted)); *see also Walker v. Fabrizio & Brook, P.C.*, 2017 WL 5010781, at *3 (E.D. Mich. 2017) (citing to *Ori* and indicating that 'takes the baton,' 'sends the information,' and 'hands it off' are all synonymous with the word 'conduit').

[23] *See Kholost v. U.S. Department of Housing and Urban Development*, 2018 WL 3539814, at *4 (E.D.N.Y. July 23, 2018) (finding that receipt and retransmission of a fraud alert from a consumer reporting agency did not make the entity retransmitting the alert a consumer reporting agency); *Zelaya v. Foot Locker, Inc.*, 2018 WL 2463624, at *6 (N.D. Cal. June 1, 2018) (declining to conclude an entity acting as a conduit between employers and the U.S. Department of Homeland Security E-Verify service was a consumer reporting agency).

[24] 2016 WL 5850362, at *4-5 (D. Ariz. 2016), appeal dismissed, 2017 WL 512 5125695 (9th Cir. 2017) (unreported opinion).

[25] *Id.* at *5 (citing to Fieldprint's Declaration which stated that "Fieldprint personnel cannot access, view, analyze, manipulate, alter, or evaluate the CHRI transmitted by the FBI to [Chase].").

[26] *Id.*

[27] *Id.* at *4 (citing to *Mattiaccio v. DHA Grp., Inc.*, 21 F. Supp. 3d 15, 23–25 (D.D.C. 2014) (finding that "attorney with a clear fiduciary and agency relationship to the employer-client at whose behest the attorney-defendant conducted a background investigation" and who was not shown to have "made the decision to terminate Plaintiff" was not a CRA); *Weidman v. Fed. Home Loan Mortg. Corp.*, 338 F. Supp. 2d 571, 575–77 (E.D. Pa. 2004) (overruled on other grounds) (finding that defendant who merely requested "credit reports on behalf of a contracting lender" in order to assist lenders in deciding whether to offer credit, acted as lenders' agent and, therefore, was not a CRA because it acted "at the behest of principals with primary control over the process of

As was discussed in the SBREFA hearings, there are a number of entities that provide important services in the consumer reporting ecosystem that have long been viewed not to be CRAs and that would be impacted by any attempt by the CFPB to rewrite the statutory definitions. For example, many lenders use loan origination platforms through which they obtain and assess data from a variety of sources – the consumer (through an application), CRAs, and other third parties (such as employers). Depending on how the CFPB redefines the terms "assemble or evaluate," these loan origination systems may fall within the definition of a CRA. Similarly, entities that obtain data from one source to retransmit it (such as Fieldprint in the example above) may fall within the definition of a CRA.

Subjecting a loan origination system to the FCRA could force the technology provider to drastically change their business model, as requirements like maximum possible accuracy standards would be imposed on the tech provider, not the data provider. It would also raise questions about whether a loan origination system takes adverse action against a consumer if it knows—for example—what a credit grantor's or investor's debt-to-income minimums are and calculates the applicant's ratios. It is unclear what problem the CFPB intends to solve here, when much of this data is consumer provided or permissioned and the practical impact would be to slow down the mortgage loan origination process.

3. "Credit header" data

The Outline states that the CFPB is considering a proposal "to clarify the extent to which credit header data constitutes a consumer report," which the CFPB notes "would likely reduce, perhaps significantly, consumer reporting agencies' ability to sell or otherwise disclose credit header data from their consumer reporting databases without a permissible purpose."[28] Any such regulation would be contrary to well-settled regulatory and judicial precedents. Further, such regulation would be burdensome and duplicative, as the use and disclosure of header information obtained from financial institutions is sufficiently regulated under the Gramm-Leach-Bliley Act (GLBA). In addition, credit headers allow for prompt verification and authentication of identities, fraud prevention, and compliance with laws and rules, such as Know Your Customer guidelines. Subjecting credit header information to the FCRA would limit protections for consumers that, in the absence of identity verification, could subject consumers to identity theft from domestic and international criminal enterprises. Businesses, nonprofits, and governments who rely on this information for fraud prevention and other socially beneficial uses would also be negatively impacted, which in turn will cause an increase in the costs of the products and services offered to consumers.

a. The FCRA and the Definition of "Consumer Report."

The FCRA regulates consumer reports. CRAs have access to a variety of information in addition to that which constitutes a "consumer report," including credit header information

obtaining consumer reports and making credit decisions").
[28] Outline at 10.

such as name, address, telephone number, and Social Security number. Information only becomes a consumer report when it is:

- a communication of information by a CRA 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 to serve as a factor in establishing the consumer's eligibility for credit, insurance, or other permissible uses.[29]

Regulators and courts are clear: Because credit header information does not bear on one of the seven § 603(d)(1) factors **and also** because it is not used, expected to be used, or collected to establish eligibility for an FCRA-permissible purpose, credit header information is not a consumer report. The law does not support a different interpretation.

Thus, the sale or purchase of credit header information is not the sale or purchase of a consumer report because credit header information inherently serves a different purpose (*e.g.,* to validate that a person is who the person claims to be) from a consumer report (*e.g.,* the person is or is not creditworthy or otherwise eligible for the product or service). Therefore, all categories of credit header data should be **excluded** as a consumer report.

b. Courts Have Consistently Held That Credit Header Information Is Not Regulated under the FCRA.

Federal courts have consistently found that identifying information is not "bearing on" information essential to characterizing a communication as a consumer report. For example, in *Parker v. Equifax Information Services, LLC*, the court considered whether the Equifax product "eIDcompare" that was used solely to verify the identity of a consumer was a "consumer report" under the FCRA.[30] The Plaintiffs alleged that the eIDcompare product receives from its subscribers' data packets that include fields for a consumer's name, phone number, Social Security number, date of birth, driver's license, current address, and time spent at that address.[31] However, the court explained that "[t]he accumulation of biographical information from Equifax's products **does not constitute a consumer report** because the information does not bear on Parker's credit worthiness."[32] Further, "[t]he data at issue here reflects biographical information generally recognized as header data and, thus, **is not a consumer report**."[33] The Sixth Circuit made a similar pronouncement in *Bickley v. Dish Network, LLC*, stating that

[29] *See gen*. FCRA Section 603(d)(1).
[30] No. 2:15-CV-14365, 2017 WL 4003437, at *3 (E.D. Mich. Sept. 12, 2017).
[31] Id. at *2.
[32] Id. at *3 (emphasis added).
[33] Id. (emphasis added).

"header information" is not a consumer report.[34] Multitudes of other federal courts, as recently as last month, have stated the same.[35]

c. Congress and Federal Agencies Have Long Recognized That Credit Header Information Is Not Consumer Report Information.

The FTC's long-standing and unambiguous interpretation of the FCRA is that identifying information (*i.e.*, credit header information) does not constitute a consumer report.[36] Further, the FTC has formally adopted a reading of the FCRA that identity verification products (which rely upon such credit header information) are not "consumer reports" under the FCRA.[37] The FTC recognized that the GLBA, not the FCRA, governs credit header information. This determination is also reflected in the supplemental information to the final GLBA rule: "[t]o the extent credit header information is not a consumer report, it is not regulated by the FCRA." The FTC excluded from the 2009 Furnisher Rule any direct disputes related to the consumer's identifying information, "such as name(s), date of birth, Social Security number, telephone number(s), or address(es)."[38] This exclusion reinforces the position that such information is not regulated by the FCRA.

---

[34] 751 F.3d 724, 729 (6th Cir. 2014).

[35] *See Gray v. Experian*, No. 8:23-cv-981-WFJ-AEP, 2023 WL 6895993 (M.D. Fla. Oct. 19, 2023); *see also Trans Union Corp. v. FTC,* 81 F.3d 228, 229, 231–32 (D.C. Cir. 1996) (rejecting the view that "any scrap of information transmitted to credit grantors as part of a credit report must necessarily have been collected" for one of the three purposes listed in the definition of "consumer report"); *Individual Reference Servs. Group v. FTC*, 145 F. Supp. 2d 6, 17 (D.D.C. 2001) (name, address, Social Security Number, and phone number do not bear on required factors); *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); *Dotzler v. Perot*, 914 F. Supp. 328, 330 (E.D. Mo. 1996) (name, current and former addresses, and Social Security Number do not bear on factors); *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. Trans Union*, 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) (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.").

[36] *In the Matter of Trans Union Corp.*, FTC Docket No. 9255 at 30 (Feb. 10, 2000) (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").

[37] *See* July 29, 2008 letter to Marc Rotenberg, p. 1, n.1 (distinguishing a prior settlement on the basis that it merely involved an identification verification product, not a consumer report), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reedrotenbergletter.pdf.

[38] *See* 12 C.F.R. § 1022.43(b)(1)(i); *see also* "Consumer Reports: What Information Furnishers Need to Know," FTC Business Guidance (June 2013) *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-

Congress has also recognized that identity verification and fraud prevention products built using credit header information are not regulated under the FCRA. The Dodd-Frank Act gave the CFPB jurisdiction over consumer financial products or services, including credit reporting, but carved out from the definition of "financial products or services" those used for identity authentication or fraud or identity theft detection, prevention, or investigation, signaling that identity verification products that rely on credit header data are not covered by the FCRA.[39] In fact, in a report about the consumer reporting industry, the CFPB itself called out the unique nature of credit header information, stating that the "header of a credit file contains the identifying information of the consumer with whom the credit file is associated including an individual's name (and any other names previously used), current and former addresses, Social Security number (SSN), date of birth, and phone numbers."[40]

d. Credit Header Information from Financial Institutions Is Fully and Appropriately Regulated under the GLBA.

The GLBA strictly regulates the use and disclosure of credit header information from financial institutions. The GLBA provides consumers with notice and opt-out rights. Under that Act, a financial institution must inform consumers of that institution's data-sharing practices. Consumers are empowered with the right to opt out of information-sharing unless such sharing is permitted under certain defined exceptions. Those exceptions apply to various types of information-sharing necessary for processing or administering a financial transaction requested or authorized by a consumer. This includes, for example, disclosing credit header information to service providers that mail account statements and perform other administrative activities for a consumer's account.

The exceptions also apply to other beneficial types of information-sharing, including disclosures for purposes of preventing fraud, responding to judicial process or a subpoena, and complying with federal, state, or local laws. Examples of appropriate information disclosures under this exception include those made to technical service providers that maintain the security of consumer data, to attorneys or auditors, to the purchaser of a portfolio of consumer loans, and to a CRA consistent with the FCRA. The GLBA also restricts the reuse and redisclosure of information shared by a nonaffiliated entity under these exceptions. Entities receiving such information (whether or not they are financial institutions) may only disclose and use the information in the ordinary course of business to carry out the purpose for which it was received.

0118_consumer-reports-what-information-furnishers-need-to-know_2018.pdf.

[39] 12 U.S.C.A. § 5481(15)(B)(i). *See also Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Consumers* (March 2012), at 67, *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[40] "Key Dimensions and Processes in the U.S. Credit Reporting System," CFPB Report, p. 8 (December 2012), *available at* https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.

To protect consumers, CDIA members have adopted robust procedures. CRAs confirm that the entities receiving credit header data under the GLBA exceptions obtain such information for the purposes permitted under the exceptions. Further, CRAs contractually require such recipients to only reuse and redisclose the information consistent with those purposes.

e. Credit Header Data Serves Many Beneficial Functions That Would Be Lost If the Data Were Subject to the FCRA.

Extending FCRA requirements to credit header information contradicts 50 years of law and policy. Such extension would also unnecessarily restrict the beneficial uses of credit header information, thus harming consumers and commerce generally. This is because the many important and beneficial uses of credit header information may not constitute a "permissible purpose" under the FCRA.

Credit header data uses are essential to the public interest. Many of the socially beneficial uses for header data were outlined in CDIA's Comment to the CFPB in connection with the CFPB's Request for Information on Data Brokers and Other Business Practices (RFI). CDIA encourages the CFPB to review those comments, some of which are amplified here.

One example of the value of credit header data is the use of Social Security numbers "in identifying and locating missing family members, owners of lost or stolen property, heirs, pension beneficiaries, organ and tissue donors, suspects, witnesses in criminal and civil matters, tax evaders, and parents and ex-spouses with delinquent child or spousal support obligations."[41] Outside of an FCRA eligibility permissible purpose, credit header information also:

- is used to locate missing and exploited children and to investigate human trafficking;[42]
- helps to locate parents who have evaded child support enforcement;[43]
- helps to proactively identify and locate victims of natural disasters;
- is used by shipping carriers to ensure that packages are sent to the correct address;

---

[41] *See generally* Hearing on Enhancing Social Security Number Privacy: Before the Subcomm. on Social Security of the House Ways and Means Comm. Subcomm. on Social Security, June 15, 2004 (107th Cong.) (statement of Prof. Fred H. Cate, Indiana University School of Law).

[42] In November 2020, a missing 15-year-old girl in Austin, Texas "was one of nearly 200 children who've been safely recovered through the [National Center for Missing & Exploited Children's] ADAM Program." The Automated Delivery of Alerts on Missing Program was built by the NCMEC's "long-time partner" and CDIA member, LexisNexis® Risk Solutions. NCMEC Blog, Revolutionizing the Search For Missing Kids, Nov. 20, 2020.

[43] Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the "deadbeat parents" they sought. Information Privacy Act, Hearings before the Comm. on Banking and Financial Services, House of Representatives, 105th Cong., 2nd Sess. (July 28, 1998) (statement of Robert Glass).

- is used by insurance carriers in claims investigations to locate responsible parties and witnesses;
- is used in the legal industry to locate witnesses and serve legal process;
- expedites the reunification of lost assets with rightful beneficiaries;[44]
- reduces the risk of identity theft as it is used by financial institutions to comply with Know Your Customer guidelines;
- is employed by sellers to prevent online purchase fraud and reduce the risk of consumer victimization or to ensure age-restricted content is not available to minors; and
- enables law enforcement to investigate crimes, to exonerate innocent suspects, and to locate victims, witnesses, terrorists, and fugitives.

In another of many examples, CDIA members offer fraud prevention and detection services to prevent fraud on businesses, consumers, and third parties. These services may 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. Fraudsters are always looking for new avenues to infiltrate systems and data, perpetuate identity theft, and create synthetic identities. Therefore, access to credit header information is crucial to administer fraud detection and prevention services effectively.

President Biden reflected the nation's distress over the "historic degree of outright fraud and identity theft of [pandemic] benefits" and issued "a three-part historic Pandemic Anti-Fraud proposal."[45] The President prioritized consumer protections by announcing an "...invest[ment] in better prevention of identity theft and all forms of major fraud involving public benefit programs," and working to "[ensure] resources [and] time for investigations and prosecution of those engaged in major or systemic pandemic fraud."[46] Fraud detection and prevention services not only directly protect consumers and businesses, but by protecting consumers and businesses, such products also promote competition and help keep costs lower for consumers and small businesses. Small businesses with fewer resources that rely on these services are disproportionately at risk for fraud, so ensuring the availability of fraud detection and prevention products supports small businesses and startups, furthering competition. Small

---

[44] The presence of an SSN increases the chance of locating a pension beneficiary from less than 8 percent to more than 85 percent. *Hearing on Protecting Privacy and Preventing Misuse of Social Security Numbers before the Subcomm. On Social Security of the House Comm. on Ways and Means*, May 22, 2001 (statement of Paula LeRoy, President, Pension Benefit Information).

[45] The White House, *FACT SHEET: President Biden's Sweeping Pandemic Anti-Fraud Proposal: Going After Systemic Fraud, Taking on Identity Theft, Helping Victims*, available at https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-president-bidens-sweeping-pandemic-anti-fraud-proposal-going-after-systemic-fraud-taking-on-identity-theft-helping-victims/.

[46] *Id.*

businesses also have fewer resources to build internal fraud detection and prevention tools, so they rely on third-party providers. Thus, restricting access to credit header information necessary to help businesses prevent identity theft and fraud would disproportionately impact smaller market participants. In addition, decreasing the ability to detect fraud will lead to greater credit and fraud losses, with these increased risks and associated costs passed to consumers and small businesses.

f. The Potential Downstream Effects of Regulating Credit Header Information as Consumer Report Information are Real and Harmful to Consumers.

If credit header information is considered consumer report information and if CRAs are required to apply the same procedures to credit header information as they do to a consumer report, consumers will be harmed. For example, credit header information may then be subject to state security freeze laws, which in turn means that the credit header information will not be available for basic consumer authentication absent a consumer lifting the freeze. Therefore, businesses would be forced to require consumers to lift their security freeze each time the business needs to authenticate the consumer. Freezing and unfreezing of a credit file repeatedly is an extra step that could wear on consumers and serve as a deterrent to consumers to place a security freeze in the first place, exposing them to increased chances of experiencing fraud. At a minimum, it would deprive consumers of the benefit of their security freezes until they take action to reinstate the freezes after being authenticated; doubtlessly, some consumers with a legitimate need for the freezes will simply fail to reinstate them. This deterrence is counter to the advice often given by government agencies and entities that suffer a security breach.[47]

Similarly, many fraud products that leverage credit header information look for patterns in newly-supplied application information in a way that is not consistent with the accuracy requirement under the FCRA, but which products operate to protect consumers from identity theft. For example, these fraud products can identify where multiple persons are using the same Social Security number, where the same mobile telephone number is showing up associated with multiple, otherwise unrelated consumers, etc. If the FCRA accuracy requirement were applied to these products, the products could only use information that has been verified to belong to the consumer – which would destroy the ability of the product to flag fraud.

Additionally, if credit header information is considered consumer report information, businesses will be forced to use alternative, and less comprehensive, accurate, and current, sources of data, such as public records, to verify the identity of their customers. Public records may include real estate transaction records, criminal records, tax liabilities, civil liens, sex offender registries, bankruptcies, and other forms of information made publicly available

[47] *See, e.g.*, FTC, *What to Know About Credit Freezes and Fraud Alerts*, available at https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts (May 2021).

usually by a state or local agency. Not every consumer has a public record. Thus, a business will see a significant decrease in the number of consumers that the business is able to validate. Consequently, consumers may see a significant increase in the amount and type of personally identifiable information that consumers must prove on their own (*e.g.,* presentation of driver's license, current utility bill, Social Security card) to enter into a financial transaction.

Furthermore, given the higher rate of fraud in certain vulnerable populations, the removal of credit header information from available means of identity verification and other uses not covered by the FCRA likely will affect the underserved, the elderly, younger consumers including students, military members, and consumers of lower-socioeconomic statuses. This concern is exacerbated for consumers who do not have alternate forms of identification, such as a driver's license or state-issued identification document. According to the Department of Justice, "at least one-third of identity theft victims live in lower-income households."[48] According to the FTC, "about a third (385,590) of reports [in the calendar year 2022] that included age information came from people 60 and older, and their reported losses totaled more than $1.6 billion. Because the vast majority of frauds are not reported, these numbers include only a fraction of older adults harmed by fraud."[49] The FTC has also suggested that "servicemembers are experiencing highly disproportionate instances of theft from their financial accounts compared to the general population."[50] The removal of credit header data may be felt most by vulnerable populations.

To benefit consumers, to help prevent fraud, to avoid unintended costs and consequences, and for many other socially beneficial reasons, CDIA requests that the CFPB take no action that purports to regulate credit header information in a manner contrary to existing law, regulatory guidance, and well-settled legal precedent.

4. Targeted marketing and aggregated data

In this section of the Outline, the CFPB expresses concern about the use of consumer report data for marketing, suggesting that CRAs may be delivering advertisements on behalf of third parties to defined sets of consumers under the belief that no consumer report has been furnished to such third parties.[51] The Outline, however, provides no further detail about why the CFPB believes that information has been shared with a third party (an element of the definition of a CRA) under the hypothetical it sets forth, nor does the CFPB explain the

---

[48] Greene, Sara S., *Stealing (Identity) From the Poor*, *Minnesota Law Review* https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=4343&context=mlr#:~:text=Results%20from%20the%202016%20Department,a%20problem%20for%20several%20years. (2021) [internal citation removed].
[49] *See* FTC, *Protecting Older Consumers 2022-2023*, https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf, p. 25 (Oct. 18, 2023).
[50] FTC, *Consumer Data Spotlight: Identity Theft Causing Outsized Harm to Our Troops*, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2020/05/identity-theft-causing-outsized-harm-our-troops (May 21, 2020).
[51] Outline at 11.

prevalence or scope of this issue. For that reason, CDIA is unable to provide meaningful comments on this proposal.

Similarly, the CFPB expresses concern about the use of aggregated data for marketing purposes. The CFPB is considering proposals to "clarify whether and when aggregated or anonymized consumer report information constitutes or does not constitute a consumer report."[52] Again, beyond this statement, the CFPB does not explain how it intends to draw such lines, and without more, CDIA is unable to provide meaningful comments on the proposal. As noted by the SERs, however, the suggestion that aggregated or anonymized data could be considered a consumer report may have far-reaching implications that would severely curtail many non-marketing uses of aggregated credit data.

The FCRA defines a consumer report as "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 in whole or in part **for the purpose of serving as a factor in establishing the consumer's eligibility** [for an FCRA purpose]."[53]

Aggregated data does not meet at least two elements of this definition. To begin with, aggregated data is not used to establish a consumer's eligibility for credit or any other FCRA permissible purpose. A decision out of the Ninth Circuit, *Tailford v. Experian Information Solutions, Inc*., is instructive here.[54] In *Tailford*, the plaintiffs argued that aggregated consumer file data constituted a consumer report because the data was used to identify consumers for invitations to apply for credit.[55] Quoting the district court from which the case was appealed, Experian countered that "merely using 'information to identify a pool of potential credit applicants is not the same as using information to determine credit eligibility.'" The Ninth Circuit agreed, concluding that the use of aggregated data for targeted marketing purposes "is not using that information to establish a consumer's eligibility for credit" or any other FCRA purpose and therefore does not meet the FCRA's definition of a "consumer report."[56]

Further, aggregated data is not a consumer report because it is not "on" a particular consumer or otherwise about an identifiable consumer.[57] This reasoning is in keeping with historical FTC guidance. Previously, the FTC issued guidance stating, essentially, that data that was "coded" by identification numbers (Social Security numbers, driver's license numbers, or account numbers) were not consumer reports until they were "decoded." This decoding generally occurred at the point of delivery, *i.e.*, when the data was linked to a particular

---

[52] *Id*.
[53] 15 U.S.C. § 1681a(d).
[54] 26 F.4th 1092 (9th Cir. 2022).
[55] *See id.* at 1103.
[56] *Id.*
[57] *See* 15 U.S.C. § 1681a(d)(1); *McCready v. eBay, Inc.*, 453 F.3d 882 (7th Cir. 2006) (holding that a consumer under the FCRA must at a minimum "be an identifiable person").

consumer in connection with a particular use. For example, if a consumer provided their bank account number or Social Security number, and then that number was used to obtain information that was used to determine the eligibility of the consumer, the information would be considered a consumer report when it was delivered. However, the FTC (in its 1990 Commentary) stated that "as long as the consumer's identity is not disclosed, [coded data] are not 'consumer reports' until decoded."[58]

The FTC staff revisited this guidance in its staff report on the FCRA in July 2011 ("Forty Years Report"). The Forty Years Report noted that "[g]iven advancements in technology and the public availability of a broad range of data about consumers, staff is concerned the examples of 'coding' referenced in the 1990 Commentary – particularly coding based on Social Security numbers – could today lead to the disclosure of a consumer's identity." Based on that concern, the FTC staff clarified that information may constitute a consumer report even if it does not identify the consumer by name if it could "otherwise reasonably be linked to the consumer."[59] Aggregated data cannot be linked to a consumer.

The use of ZIP Code aggregated credit information for non-FCRA purposes is well established in both the private and public sector. For example, the credit score and insurance score studies conducted by the Federal Reserve and the FTC both relied on aggregated score information based on ZIP Codes. Further, the CFPB routinely uses aggregated credit report information for its research purposes, such as in its study on credit invisibility.

Further, anonymized credit data is used by score developers and modelers to gain insight and train models. Financial institutions use anonymized credit data sets to evaluate their internal underwriting criteria, to research and develop products, to identify trends in consumer use of credit for product development and modification, to assess portfolios, and even to design prescreen campaigns (where identifiable data is subsequently shared pursuant

---

[58] 55 Fed. Reg. 18804 (May 4, 1990).

[59] CDIA notes that in a footnote in its 2016 report on Big Data, the FTC suggested that even if data did not identify a **specific** consumer, it might constitute a consumer report if it is used in part to determine eligibility:

> In 2011, FTC staff issued the 40 Years FCRA Report. In that report, staff stated that "[i]nformation that does not identify a specific consumer does not constitute a consumer report even if the communication is used in part to determine eligibility." 40 Years FCRA Report, supra note 80, at 20. The Commission does not believe that this statement is accurate. If a report is crafted for eligibility purposes with reference to a particular consumer or set of particular consumers (e.g., those that have applied for credit), the Commission will consider the report a consumer report even if the identifying information of the consumer has been stripped.

FTC Big Data Report at pp. 16-17, n. 85. The Big Data Report, however, did not provide any further guidance as to when data about a "set of consumers" would be considered sufficiently linkable to the individual consumers such that it would be considered a consumer report. Further, this suggestion presupposes that the "report is crafted for eligibility purposes."

to a permissible purpose).[60] Depending on the nature of the CFPB's proposal, each of the important and necessary uses of aggregated or anonymous credit data may be implicated.

B. Permissible purposes

1. Written instructions of the consumer

The Outline indicates that the CFPB is considering addressing "what is needed" for a CRA to provide a consumer report in accordance with the written instructions permissible purpose. The Outline, however, lacks any specific proposals, noting only that the CFPB is considering "proposals concerning the steps companies must take to obtain a consumer's written instructions, who can collect written instructions, limits on the scope of authorization to ensure the consumer has authorized all uses of the consumer's data (including limits on the number of purposes or entities that can be covered by a single instruction), and methods for revoking any ongoing authorization."[61] Again, the lack of specificity makes it difficult to comment meaningfully.

CDIA notes, however, that FCRA permits an end user to obtain a consumer report on a consumer "in accordance with the written instructions to whom it relates,"[62] and that permission alone is sufficient; the FCRA does not need to demonstrate any other form of permissible purpose (such as a credit transaction).[63] Under existing guidance from the FTC staff, entities that obtain "written instructions" understand that it is important that the consumer's intent is clear. As the FTC staff explained in their Forty Years report:

---

[60] Further, we note that in its 2014 report on data brokers, the FTC observed that marketing lists often identify consumers who share credit characteristics, but that fact alone did not turn such information into credit reports when used for a non-FCRA marketing:

> Marketing lists identify consumers who share particular characteristics (e.g., all persons living with at least two children, all persons who are both women and own a specific car brand, people interested in diabetes, and households with smokers in them). The client identifies the attributes that it would like to find in a consumer audience, and the data broker provides a list of consumers with those attributes. A client, for example, can request a list of consumers who are "Underbanked" or "Financially Challenged" in order to send them an advertisement for a subprime loan or other services.

FTC Data Broker Report at p. 28. The FTC went on to note that "[e]ven though these categories may implicate creditworthiness, the use of data about a consumer's financial status in order to send the consumer targeted advertisements is generally not covered by the FCRA, unless the advertisements are for certain pre-approved offers of credit [i.e., an FCRA purpose]." *Id.* at p. 25 at n. 58.

[61] Outline at 12-13.

[62] 15 U.S.C. § 1681b(a)(2).

[63] The reverse is also true; written instructions, or a written consent are generally not required where a permissible purpose otherwise exists. "Generally, when permissible purposes other than employment exist, CRAs may furnish consumer reports without a consumer's specific permission or authorization." Forty Years Report, p. 42.

> A consumer's written consent qualifies as an "instruction" that provides a permissible purpose under this section if it clearly authorizes the issuance of a consumer report on that consumer. For example, a consumer's clear and specific written statement that "I authorize you to procure a consumer report on me" provides a permissible purpose under this section. However, the consumer's signature on a form that includes the statement "I understand that where appropriate, credit bureau reports may be obtained" is not a sufficiently specific instruction from the consumer to authorize a CRA to provide a consumer report. This language is more in the nature of a notification that a consumer report might be procured, as opposed to a grant of permission to obtain the consumer report.[64]

Industry has developed standards for the collection of, and reliance on, a consumer's written instructions that has served consumers well. The written instruction permissible purpose has been used to gain permission to use credit report information to help consumers shop for credit without an impact to their credit score (such as platforms that present prequalified credit offers) or to provide the consumer with access to, and education on, their credit. Written instruction also has been used in connection with transactions where the consumer's credit may need to play a role but where there is no clearly-defined permissible purpose (such as a small business loan where the consumer will not be financially liable). Without understanding better the concerns to be addressed, in light of existing guidance and the beneficial uses described above, CDIA contends that no further clarification is required.

2. Legitimate business need

With respect to the "legitimate business need" permissible purpose, the CFPB sets forth two specific proposals: (1) to require under FCRA section 604(a)(3)(F)(i) that a transaction needs to have been initiated by the consumer "for personal, family, or household purposes" and to permit the use of consumer reports only for the purpose of determining the consumer's "eligibility" for the business transaction, and (2) to limit the use of FCRA section 604(a)(3)(F)(ii) in an account review for which the use of a consumer report is actually needed to make a decision about whether the consumer continues to meet the terms of the account. Although CDIA appreciates the specificity of the proposal here, both are contrary to the plain language of the FCRA and fall outside of the CFPB's rulemaking authority.

The statute provides that there is a permissible purpose to furnish a consumer report where a person "has 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."[65] To this language, the CFPB proposes to read in a non-statutory requirement that requires that the transaction was initiated by the consumer for "personal, family, or household purposes" and such reports may be used "only for the purpose of determining the customer's eligibility for

[64] Forty Years Report p. 43.
[65] 15 U.S.C. § 1681b(a)(3)(F).

the business transaction." The agency further proposes that, for account reviews, the consumer report must be "actually needed to make a decision about whether the consumer continues to meet the terms of the account."[66]

Congress spoke clearly when it enacted the FCRA – where the statute's coverage is limited to "personal, family, or household purposes," it knew how to say so, as for adverse action notices based on information from entities that are not CRAs.[67] Here, though, the legitimate business need permissible purpose has no such limit in its language – and the CFPB's proposal seeks to impermissibly overwrite Congress' clear language.

Based on established FTC guidance and case law, the consumer reporting system has developed several use cases under this permissible purpose where the transaction is "initiated' by the consumer:

- Applying to rent an apartment, offering to pay goods with a check, or applying for a banking or brokerage account.[68]
- Applying for provisional checking accounts and similar financial services.[69]
- Evaluating risk of delayed payments to small businesses (dentists).[70]
- Furnishing a consumer report where the CRA has reason to believe that a business transaction was initiated by the consumer, even if subsequently the transaction was found to involve identity theft.[71]
- Leasing or renting a car without requiring the consumer to reveal whether the lease is for business or personal use. Here, a car rental agency may pull a consumer report to evaluate the degree of risk posed by the consumer renter before the agency permits them to drive off the lot with a valuable asset.

The Outline would limit these cases and reduce consumer privacy, were it to require that end users query consumers and use different authorizations and transaction accounts, depending on whether an apartment lease was corporate or residential, an auto rental was for vacation or business use, and a deposit/brokerage/checking account opening was for personal, family, or household purposes or for some other purpose. Introducing new transactional complexity without corresponding consumer benefit, as the CFPB proposes here, is a step backward for consumers and business alike – and is not required by the FCRA.

---

[66] Outline at 13.
[67] "Whenever credit for personal, family, or household purposes involving a consumer is denied or the charge increased...,"15 U.S.C. § 1681m(b)(1).
[68] *See* Forty Years Report 604(a0(3)(F) items 3B, 3C,3D.
[69] FTC Staff opinion Letter, Feb 5, 1985.
[70] *Wallace v. Finkel*, 2006 WL 1731149 (M.D. Ala. June 22, 2006).
[71] *Bickley v. Dish Network*, 754 F.3d 724 (6th Cir. 2014).

3. Data security and data breaches

The CFPB is considering a proposal to address a CRA's obligation to protect consumer reports from a data breach or unauthorized access under the FCRA, including making the failure to protect against unauthorized access to consumer reports by third parties a violation of section 604 or 607(a) of the FCRA. The CFPB is also asking for feedback regarding the data security improvements and associated costs CRAs would incur if they were liable for all such data breaches under the FCRA.

The CFPB's proposal to make certain data breaches a violation of the FCRA is both unwarranted and redundant given existing statutory and regulatory requirements. The Safeguards Rule, promulgated under GLBA, requires financial institutions, including CRAs, to implement and maintain certain controls to protect the security, integrity, and confidentiality of consumer data. Specifically, the Safeguards 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. In August 2022, the CFPB issued Consumer Financial Protection Circular 2022-04 in which the CFPB stated that failure to implement and maintain adequate information security practices as required under the Safeguards Rule is an unfair practice under the Consumer Financial Protection Act.[72] Data security controls, above and beyond those already required by the Safeguards Rule, are not necessary.

Both federal and state regulators have ample avenues available to address perceived data security failures. In September 2021, the CFPB published information technology examination procedures to be used by examiners "to assess IT and IT controls as part of a CMS review," indicating that the CFPB would evaluate a covered entity's data security practices as part of the typical examination process.[73] State laws and regulations also require many users of consumer reports, such as financial institutions and insurance providers, to adequately safeguard consumer information and/or expressly require compliance with the Safeguards Rule.[74] A review of existing regulatory enforcement actions reinforces that any number of state and Federal agencies already have the ability to enforce data security practices, rendering an additional enforcement authority unnecessary. For example, in 2011, the FTC took action against three credit report resellers alleging that the companies did not take reasonable information security steps to protect consumer data and therefore violated

---

[72] https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf. CDIA takes no position on whether this legal interpretation is correct; it just notes that the Bureau itself has already recognized that the Safeguards Rule protects consumer data in this way.

[73] https://www.consumerfinance.gov/compliance/supervision-examinations/compliance-management-review-information-technology-examination-procedures/.

[74] *See e.g.*, Ga. Comp. R. & Regs. 80-11-1-.08 (requiring mortgage brokers, lenders, and servicers to comply with the Safeguards Rule); Mich. Admin. Code R 500.551 *et seq.* (requiring insurance licensees to develop and implement an information security program); 23 NYCRR 500 (imposing cybersecurity requirements for financial services companies).

the FTC Act, the FCRA, and the GLBA.[75] In 2017, the FTC and CFPB along with 50 state attorneys general took action against Equifax for alleged data security failures.[76] In May 2023, the New York Department of Financial Services entered into a consent order with OneMain Financial, a consumer lender and mortgage servicer, to address its alleged failure to comply with New York data security regulations identified during an examination and subsequent enforcement investigation.[77] These actions demonstrate that neither federal nor state regulators have been hindered in enforcement with respect to data security, without the need to engage in additional FCRA rulemaking.

The CFPB alleges that "unauthorized users have gained access to consumer reports maintained by consumer reporting agencies on a number of occasions."[78] As a predicate to the CFPB's allegations, the CFPB appears to erroneously insinuate that CRAs do not adequately verify end users' permissible purposes. The fact that a threat actor has infiltrated a system does not establish that the CRA furnished a consumer report without a permissible purpose. CRAs are required to maintain reasonable procedures designed to limit the **furnishing** of consumer reports to section 604 permissible purposes, as the CFPB recites in its proposals.[79] Among other controls including audits of end users' actual use of consumer report information, CRAs have established reasonable procedures to identify end users and verify the end users' identity pursuant to section 607, require end users to certify to the end users' applicable permissible purpose, and require end users to protect consumer report information with adequate security controls. Additionally, courts have held that stolen data does not constitute the furnishing of a consumer report under the FCRA — "Although 'furnish' is not defined in the FCRA, courts generally use the term to describe the active transmission of information to a third-party rather than a failure to safeguard the data."[80] Moreover, it is difficult to address the CFPB's exact concern because additional details related to the purported unauthorized users' access are not provided. And a review of the FTC actions involving data security practices over the last several years demonstrates that the vast majority of data breaches that have been the subject of enforcement actions did not involve information obtained from a consumer report. Instead, these actions involved information

---

[75] https://www.ftc.gov/sites/default/files/documents/cases/2011/02/110209acranetcredit.pdf.
[76] https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf.
[77] https://www.dfs.ny.gov/system/files/documents/2023/05/ea20230524_co_onemain.pdf.
[78] Outline at 14.
[79] "Furnish" means "to provide" or "equip." It is a transitive verb, so it requires the subject, in this case the CRAs, to take some affirmative act. When a CRA is the victim of an intrusion by a hostile actor, it is not affirmatively providing or equipping those actors with consumer reports, which is the only activity the FCRA regulates.
[80] *In re Experian Data Breach Litig.*, No. SACV151592AGDFMX, 2016 WL 7973595, at *2 (C.D. Cal. Dec. 29, 2016), *citing Dolmage v. Combined Ins. Co. of Am.*, 2015 WL 292947, at *3 (N.D. Ill. Jan. 21, 2015). *See also In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1312 (N.D. Ga. 2019); *Strautins v. Trustwave Holdings, Inc.*, 2014 WL 960816, at *8 (N.D. Ill. Mar. 12, 2014); *Holmes v. Countrywide Fin. Corp.*, 2012 WL 2873892, at *16 (W.D. Ky. Jul. 12, 2012).

provided by consumers to businesses in connection with the provision of a variety of products and services ranging from home security to healthcare.[81]

The CFPB's proposal would have devastating financial consequences for SERs and other CRAs in the credit reporting system. According to a 2022 study by IBM, the average cost incurred by a company in the United States as a result of a data breach was $9.44 million.[82] Imposing additional liability on CRAs above the millions in costs they will already incur to investigate, respond to, and remediate a data breach could place SERs in an untenable financial situation. While errors and omissions (E&O) and cyber insurance was once thought to aid small businesses in controlling financial ruin in the event of a cyber incident, under the current regulatory environment, the availability of E&O and cyber insurance coverage is almost nonexistent and costly, where available. A 2023 whitepaper on the state of cyber insurance found that 79% of survey respondents experienced a rate increase upon application or renewal, with 67% stating that cyber insurances rates increased 50-100%.[83] That same whitepaper found that cyber insurance companies are limiting coverages by expanding exclusions that voided insurance coverage.[84] Increasing liability for data incidents would make the already difficult, if not impossible, task of obtaining meaningful cybersecurity insurance coverage even more arduous. And without cyber insurance coverage, entities engaged in data breach litigation can incur damages and legal costs ranging from hundreds of thousands to millions of dollars per incident, potentially posing an insurmountable blow to a small entity's financial solvency.[85]

Finally, it appears that the CFPB is intending to include a strict liability standard with respect to a data breach or unauthorized access to consumer report information by third parties. The FCRA clearly establishes an overall "reasonable procedures" requirements for CRAs;[86] however, strict liability is not a concept currently under the FCRA (or under the Safeguards Rule). The costs of complying with a strict liability standard could be overwhelming for the industry. As discussed above, the costs of cyber insurance are skyrocketing, which means that the risk of operating as a CRA may produce a barrier to new innovation and development under a strict liability regime.

---

[81] *See* https://www.ftc.gov/legal-library/browse/cases-proceedings?sort_by=field_date&items_per_page=20&search=&field_competition_topics=All&field_consumer_protection_topics=1424&field_federal_court=All&field_industry=All&field_case_status=All&field_enforcement_type=All&search_matter_number=&search_civil_action_number=&start_date=&end_date=.
[82] *See* https://technologymagazine.com/articles/data-breaches-cost-an-average-9-44m-in-the-us-last-year.
[83] Delinea Whitepaper, 2023 State of Cyber Insurance Report (on file with author); *see also* https://www.technewsworld.com/story/cyber-insurance-costs-rising-coverages-shrinking-report-178569.html.
[84] *Id.*
[85] Cybersecurity & Infrastructure Security Agency, Cost of a Cyber Incident: Systematic Review and Cross-Validation, Oct. 26, 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf; *See also* https://www.f5.com/labs/articles/cisotociso/breach-costs-are-rising-with-the-prevalence-of-lawsuits.
[86] 15 U.S.C. § 1681(b).

C. Disputes

The CFPB's proposal contemplates changes to the dispute resolution process established by the FCRA, which would impact furnishers and CRAs alike. First the CFPB proposes to adopt a rule to clarify that all disputes must be reinvestigated, whether they raise questions of fact or law – a proposal that appears wholly unnecessary given the SERs' testimony that they investigate all disputes. Second, the CFPB lacks legal authority to adopt a rule that is intended to supersede the decisions of several circuit courts who have interpreted the same FCRA section (section 611(b)).

1. Disputes involving legal matters

The CFPB has expressed two concerns that seem to underpin the Outline related to legal versus factual disputes. The first is a concern that CRAs are willfully avoiding their obligations under the FCRA to investigate a dispute on the basis that the dispute raises a pure legal issue. The second concern is the belief that the various circuit and district courts that have examined the issue have erred in their interpretation of the FCRA, and the CFPB believes it has authority to correct the courts' legal analyses.

First, every CRA SER explained that they handle all disputes, regardless of the stated basis of the dispute, which feedback clearly belies the concern. The SERs explained that they reinvestigate the dispute "as far as they can," but that there are times when what is presented as a credit report dispute is beyond their ability to resolve – such as where it raises a legal challenge to the validity of a debt. In explaining why a legal challenge to the validity of a debt is not something a CRA can resolve in the context of a dispute reinvestigation, the SERS reported being ill-equipped to handle such reviews. Moreover, SERs would be required to hire an army of lawyers to review numerous pieces of often conflicting information and make quasi-judicial legal rulings applying federal and state law raising due process concerns as well.[87] For the SERs to secure these resources would be time consuming and cost prohibitive. In response to the CFPB's follow-up questions regarding whether it would be helpful to have a definition for whether a particular dispute was a "legal dispute" versus a "factual dispute" - the CRA SERs answered, unequivocally, that it would not. The SERs stated that having to undertake such a preliminary determination would be unduly burdensome, and hinder their ability to timely complete a reinvestigation.

These are exactly the reasons why the courts that have examined the question of whether a CRA is liable to a consumer for damages under the FCRA for failing to conduct a reasonable investigation of a dispute that raises a legal question have answered in the negative. Requiring CRAs to act as arbiters of legal disputes in the first instance would turn the district courts into novel appellate panels, further clogging an already burdened judiciary. Not to mention the fact that consumers might be misled to believe that the CRA's

[87] It is worthy of note that courts resolve disputes after months or years of discovery, briefing, and possible trial. CRAs only have thirty days to reinvestigate disputes and do not have subpoena power.

determination carries some legal effect on the enforceability of the debt outside of credit reporting. As the Seventh Circuit in *Denan v. Trans Union* explained "neither the FCRA nor its implementing regulations impose a comparable duty upon consumer reporting agencies, much less a duty to determine the legality of a disputed debt."[88] That is because a consumer must identify a factual inaccuracy in the consumer's file that can be rectified by the reinvestigation of a CRA. In *DeAndrade*, for example, the consumer argued that the furnished mortgage was invalid because the consumer never agreed to allow a lien to be placed on their home to finance the installation of their windows.[89] As the court explained "[w]hether the mortgage is valid turns on questions that can only be resolved by a court of law, such as whether DeAndrade ratified the loan. This is not a factual inaccuracy that could have been uncovered by a reasonable reinvestigation, but rather a legal issue that a credit agency such as Trans Union is neither qualified nor obligated to resolve under the FCRA."[90] Under the FCRA dispute procedures, CRAs, after assuring that the alleged inaccuracy was not the result of their own actions, are to refer disputes to the furnishers, who have more information regarding the underlying account, and are therefore in a better position to determine whether the consumer's dispute has merit. That is not to say that CRAs do, or should, ignore the consumer's dispute. However, it does mean that there is a point at which the work of the CRA must stop and the work of the courts must begin.

Further, simply because the CFPB does not agree with the outcome of these cases does not mean it has the legal authority to change what the courts have declared the law to

---

[88] *Denan v. Trans Union LLC*, 959 F.3d 290, 295 (7th Cir. 2020). The Seventh Circuit is by no means standing alone on this issue. In fact, at least seven circuit courts have applied the collateral attack doctrine to hold that the FCRA does not impose civil liability on a CRA where the dispute really raises a legal challenge to the validity of a debt or other account. *Mader v. Experian Info. Sols, Inc.,* 56 F.4th 264 (2d Cir. 2023) (holding that the kind of legal inaccuracy alleged by Plaintiff is not cognizable as an "inaccuracy" under the FCRA); *Batterman v. BR Carroll Glenridge, LLC*, 829 F. App'x 478, 481 (11th Cir. 2020 (finding plaintiff's theory of inaccuracy was actually "a contractual dispute" to be resolved by a court and not a CRA) (per curiam); *Wright v. Experian Info. Sols., Inc.*, 805 F.3d 1232, 1242 (10th Cir. 2015) (providing that FCRA's reinvestigation provisions "do[] not require CRAs to resolve legal disputes about the validity of the underlying debts they report"); *Okocha v. Trans Union LLC*, 488 F. App'x 535, 536 (2d Cir. 2012) (affirming "well-reasoned order," including holding that plaintiff's theory of inaccuracy "is a collateral legal attack on the validity of the debt … not a factual inaccuracy") (unpublished); *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 891 (9th Cir. 2010) (explaining that "courts have been loath to allow consumers to mount collateral attacks on the legal validity of their debts" in the guise of FCRA claims against CRAs because "CRAs are ill equipped to adjudicate contract disputes," and agreeing that such claims are improper); *DeAndrade v. Trans Union LLC*, 523 F.3d 61, 68 (1st Cir. 2008) (finding plaintiff "crossed the line between alleging a factual deficiency that Trans Union was obliged to investigate pursuant to the FCRA and launching an impermissible collateral attack against a lender by bringing an FCRA claim against a [CRA]"); *Saunders v. Branch Banking and Tr. Co. of VA*, 526 F.3d 142, 150 (4th Cir. 2008) (noting that "[c]laims brought against CRAs based on a legal dispute of an underlying debt raise concerns about 'collateral attacks' because the creditor is not a party to the suit, while claims against furnishers … do not raise this consideration because the furnisher is the creditor on the underlying debt").

[89] *DeAndrade*, 523 F.3d at 68.

[90] *Id.*

be. As has long been the rule in our country "[it] is emphatically the province and duty of the judiciary to say what the law is."[91] The CFPB has no authority to adopt a rule to 'overrule' the decisions of the various circuit courts that have decided this issue; only Congress has that power.

2. Disputes involving systemic issues

The CFPB proposes another extra-statutory concept, a separate process to reinvestigate disputes relating to "systemic issues" affecting the completeness or accuracy of information in consumer reports. The Outline does not define what would amount to a "systemic issue" under the new rule, nor does it detail specific requirements. The following topics appear to be under consideration: a specific reinvestigation requirement requiring a determination whether the dispute raises a "systemic issue" that affects multiple consumers; a specific requirement to correct the issue as part of the reinvestigation process, and update reporting for all affected consumers; a requirement to provide notice to all affected consumers of the updates; requiring a specific "systemic dispute" channel through which consumers could file these specific disputes; and the creation by the CFPB of a rubric or template consumers could use to submit disputes relating to multiple consumers.[92]

This is another area where the CFPB seeks to create a new law, rather than seeking to "administer and carry out the purposes and objectives" of the FCRA or "to prevent evasions" or "to facilitate compliance." The FCRA's express dispute provisions leave no room for the CFPB to create sub-types of disputes, or separate processes and requirements for handling disputes.[93] Further, section 611 of the FCRA requires CRAs to reinvestigate disputes received "directly" from consumers. By proposing to graft on new dispute reinvestigation process and notice requirements by rule, the CFPB does not fill any gaps in a highly detailed statute. Rather, the agency proposes to rewrite the FCRA dispute process here beyond the reach of its delegated authority.

Congress has created specific procedures to handle certain types of disputes – namely, those that result from identity theft and fraud. In 2003, the FCRA was amended to provide for special rules and processes to govern reports that a consumer has suffered from identity theft and fraud.[94] Congress also amended the FCRA to create special COVID reporting requirements in Section 623 (a)(1)(F).[95] If Congress felt that there needed to be another special type of dispute, it would create one.

---

[91] *Marbury v. Madison*, 5 U.S. 137, 177, 2 L. Ed. 60 (1803) (emphasis added).
[92] Outline at 16-17.
[93] The sole precedent the agency provides for this vast, problematic new process is a single case involving Regulation V furnisher violations that continued for four years involving 80,000 furnished items. Even assuming that the CFPB had *enforcement authority* to bring the matter does not mean it has been delegated *rulemaking authority* to modify the dispute process established by Congress.
[94] Pub. L. No. 108-159, 117 Stat. 1952.
[95] 15 U.S.C. § 1681s-2(a)(1)(F).

The CFPB's failure to define "systemic" makes it nearly impossible for affected parties to comment on its impact during the SBREFA phase. Agency staff suggested anecdotally during the SERs' hearing that a systemic designation for a dispute could result from even a handful of disputes, which is really no guidance at all. Consumer dispute reinvestigations are highly fact-specific – varying with several factors, including end users' policies and actions, consumer-specific attributes, transaction documents and actions, dispute reporting processes, and applicable state law. Despite this variation, enabling consumers to designate disputes as "systemic" is likely to have one clear consequence - enabling plaintiffs' counsel in civil litigation to more easily argue commonality and/or typicality of consumers' harm under Rule 23 of the Federal Rules of Civil Procedure. This, in turn, would lead to a massive increase in FCRA class action filings, thereby overwhelming the federal courts, and unnecessarily increasing the potential costs to CRAs and furnishers.[96] This is an abuse of the CFPB's rulemaking authority.

In reality, consumers will rarely know if their dispute is part of a larger "systemic" issue, and so allowing a consumer to flag a dispute as systemic will likely result in consumers being confused about this special track for such disputes. It is not difficult to foresee that consumers and their paid agents would regularly designate a dispute as "systemic" if given the option to do so, thereby triggering more costly reinvestigation requirements, which industry must assume will likely also be more time consuming, even where the consumer has no evidence that her/his experience is part of a "systemic" issue.

And it is just as predictable that some consumers will be put off by the question of whether they believe that their dispute is systemic and fail to submit their dispute because of their confusion. Notably, the consumer reporting system has some relevant prior experience when the FTC established a new process for the creation of identity theft reports through its online identity theft complaint portal. The identity theft complaint portal created a new avenue for credit repair organizations to request blocks of information, sometimes abusively, [97] disrupting consumers' ability to access credit and properly identify themselves, and negatively affecting the quality and completeness of consumer data in the system. Industry had limited time to adjust their procedures to account for the sudden rise in fraudulent or baseless block

---

[96] FCRA litigation has been on the rise in recent years. According to WebRecon, courts saw a 3.5% increase in FCRA complaints in both 2021 and 2022. WebRecon Stats Dec '22 & Year in Review (Jan. 31, 2023), https://webrecon.com/webrecon-stats-dec-22-year-in-review/. Its most recent data, from September 2023, shows a 6.5% increase in FCRA litigation from the month prior. WebRecon Sept 2023 Stats: The Pendulum... (October 30, 2023), https://webrecon.com/webrecon-sept-2023-stats-the-pendulum/. In contrast, during the aforementioned time periods, FDCPA and TCPA complaints were significantly down.

[97] An FTC analysis of the complaints received during the first 6 months of calendar year 2021 revealed significant patterns that suggest a possible fraudulent use of IdentityTheft.gov. These patterns foretell a risk to the credibility of a high number of complaints within the system." Federal Trade Commission Office of Inspector General, *Fiscal Year 2021 Report on the Federal Trade Commission's Top Management and Performance Challenges* (Sept. 30, 2021), at p. 8, available at https://www.ftc.gov/system/files/documents/reports/final-oig-fy-2021-report-ftcs-top-management-performance-challenges/oig_fy_2021_ftc_top_management_challenges_final_report_9-30-21.pdf.

requests. Further, given the rise in block requests, industry had to work with furnishers to develop additional processes to allow furnishers to review blocked items and request recission of blocks where the basis for the block request was baseless or in error. Unfortunately, the CFPB proposal threatens to open the door once again to new attacks from credit repair using the "systemic" channel, resulting in longer reinvestigations for a wide range of disputes, thereby increasing risk that accurate information on consumers may be removed from the system, not to mention additional costs on CRAs and furnishers alike. Handling these new requirements within the dispute process will also have the entirely predictable result of extending the time needed to complete each "systemic" reinvestigation, a clear detriment to consumers.

With respect to the proposed notice requirement, this too exceeds the bounds of the CFPB's authority, as the FCRA enumerates the response owed to a consumer. Requiring CRAs and furnishers to send notices to consumers who have *not* filed a dispute will lead to consumer confusion, risk the revelation of consumer report information to third parties, and significantly increase litigation risk and costs.

D. Medical debt collection information

As a fundamental matter, the CFPB lacks authority to declare medical collection debt, or any other information, to be information that may not be contained within consumer reports. Congress has already established the scope of the contents of consumer reports,[98] and preempted further action by states to affect the same.[99] With regard to medical information, specifically, Congress has, on multiple occasions, amended the FCRA to regulate when, how, and to what extent medical information may be included in consumer reports. Given how thoroughly Congress has legislated, the CFPB has no authority to act by rulemaking.[100]

Not only is medical collection debt regulated as an "item of adverse information" subject to a limitation of reporting for seven years,[101] Congress further regulated the *substance* of medical information included in consumer reports. Relevant here, the then-enacted Section 1681c(a)(6) prohibited CRAs from including medical information that disclosed or implied details regarding a consumer's medical care in consumer reports. In 2003, Congress further legislated when a CRA may report medical information and the kind of medical account information that may be reported.[102] Most recently, in 2018, Congress again further regulated

---

[98] 15 U.S.C. §1681c.
[99] 15 U.S.C. §1681t(b)(1)(E).
[100] Under *Chevron*, courts examine "whether Congress has directly spoken to the precise question at issue." If so, "that is the end of the matter," and courts must enforce the "unambiguously expressed intent of Congress." *Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.,* 467 U.S. 837, 842–43 (1984)
[101] 15 U.S.C. § 1681c(a)(5).
[102] 15 U.S.C. § 1681b(g)(1) (generally requiring a consumer's consent to allow the reporting of medical information for employment and insurance purposes, and limiting any reporting of the financial aspects of medical account information so long as the information reported does not "provide information sufficient to infer, the specific

the reporting of adverse information, particularly the reporting of veterans' medical debt by the nationwide consumer reporting agencies ("NCRAs") and included a limitation on the earliest point in time such information may be reported, and when the NCRAs must cease reporting of such information.[103] Congress clearly views medical debt as an area of serious concern, and where it determines changes to how such information is furnished in consumer reports, Congress acts. There is simply no room for the CFPB to 'fill in' gaps, because Congress has left none.

It is also important to note that CRAs undertook their own work to modify the information provided in consumer reports to address unique issues related to delays caused by the insurance claims process. As a result of this voluntary industry work, the vast majority of medical debt was removed from consumer reports, allowing more time for insurance reimbursements to catch up to corresponding consumer debt obligations before the obligation was included on a consumer report. However, none of this voluntary initiative had to do with the predictiveness of the information.

The CFPB's proposed rulemaking stems from policy concerns regarding the U.S. healthcare system, and related insurance coverages. Congress and state legislatures are the proper fora for addressing these policy concerns; a rulemaking interpreting the text of the FCRA is not. Further, the CFPB's own study says that the medical debt information included in consumer scoring is predictive of delinquency, although not as predictive as other consumer collection accounts over the studied period.[104] Furthermore, under the CFPB's proposal, it would inherently consider all medical debt to be a result of unexpected catastrophes suffered by consumers rather than a routine, elective, or cosmetic procedure. While there may be inequities in the system of medical provisioning, the fact is the medical debts are relevant data, and provide a comprehensive, data-driven evaluation of consumers' repayment ability.[105] Rather than help consumers, the Bureau's proposal could hurt them by making underwriting

---

provider or the nature of such services, products, or devices.").

[103] 15 U.S.C. §§ 1681c(a)(7) & (8).

[104] For persons in the 2011-2013 period CFPB surveyed, for example, scores and delinquency rates tracked closely, for consumers with mostly medical or mostly non-medical collections. Figs. 2. A, B, at 13, "CFPB Data Point: Medical Debt and Credit Scores," 2014.

[105] Note that the Outline does not define "medical debt' that may be subject to a proposed rule, but this is another place where the definitions determine the scope of impact to industry and consumers alike. If drawn too broadly, compliance with the rule would be nearly impossible. For example, New York's recent bill banning medical debt sweeps into its scope credit card accounts where consumers have charged every-day household personal care items. N.Y. Gen. Bus. L. Sec. 380-a(v) "medical debt means any obligation or alleged obligation of a consumer to pay any amount whatsoever related to the receipt of health care services, products, or devices provided by a hospital licensed under article twenty-eight of the public health law, a health care professional authorized under title eight of the education law, or any ambulance service certified under article thirty of the public health law." CRAs lack any ability to determine if such purchases were made on revolving debt furnished to them, and therefore have no ability to identify which accounts may be in scope. As a practical matter, identifying and tracking such activity would be nearly impossible for furnishers as well, and could result in creditors prohibiting consumers' use of credit cards for such purchases, limiting consumers' access to such necessary items.

more difficult, and the extension of credit more risky, which in turn would either raise the cost of credit for all or curtail credit availability for those who may need it most.

* * *

We appreciate the opportunity to comment on the CFPB's Outline. As noted above, given the significance of the CFPB's proposals and the vital importance of the nation's credit reporting system, CDIA urges the CFPB to obtain broad stakeholder input on these proposals, through an advanced notice of proposed rulemaking, stakeholder meetings, and/or other open forums.

Sincerely,

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