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

P 202 371 0910

Writers email:
eellman@cdiaonline.org
Writer's direct dial: +1 (202) 408-7407

April 3, 2023

The Honorable Rohit Chopra
Director, Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: Response to request for broader regulation of, and advisory opinion regarding, credit header information

Dear Director Chopra:

On February 8, 2023, a coalition of immigrant rights, consumer rights, and privacy organizations ("consumer groups") wrote to the Consumer Financial Protection Bureau ("CFPB") about credit header information. This letter asked the CFPB to more broadly regulate credit header information and publish an advisory opinion stating that credit header information should not be excluded from regulation under the Fair Credit Reporting Act ("FCRA").[1]

I write on behalf of the Consumer Data Industry Association ("CDIA")[2] to oppose this request for three reasons:

- 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. Credit headers allow for prompt verification and authentication of identities, fraud prevention, and compliance with laws and rules, such as Know Your Customer guidelines.
- Rulemaking to make credit header information subject to the FCRA would be contrary to well-settled regulatory and judicial precedents.
- Such regulation would be burdensome and duplicative. The use and disclosure of header information obtained from financial institutions is sufficiently regulated under the Gramm-Leach-Bliley Act ("GLBA").

[1] 15 U.S.C. §§ 1681 *et seq.*

[2] CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies 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.

Credit header data uses are essential to the public interest. For example, "Social Security numbers also play a critical role 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."[3] Credit header information:

- Is deployed to locate missing and exploited children and to investigate human trafficking.[4]
- Is used to locate parents who have evaded child support enforcement.[5]
- Is applied to verify the applications of low-income consumers needing access to vital government benefits, like the Supplemental Nutrition Assistance Program ("SNAP") benefits[6] and healthcare coverage. Conversely, credit header information prevents public benefits fraud by allowing money that would otherwise be used fraudulently to return to people that qualify for assistance.[7]
- Expedites the reunification of lost assets with rightful beneficiaries.[8]
- Is employed by sellers to prevent online purchase fraud and reduce the risk of consumer victimization.
- Is positioned by law enforcement to investigate crimes and to locate victims, witnesses, and fugitives.
- Reduces the risk of identity theft because header information is used by financial institutions to comply with Know Your Customer guidelines.

---

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

[4] 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.

[5] 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).*

[6] To determine eligibility for benefits and to weed out fraud in SNAP, applicants go through a certification process, which includes a check of both public and non-public information from private companies. Errors and fraud in SNAP "can add up quickly and create a serious payment accuracy problem for state." The "data matching and certification process may also provide information useful in detecting recipient application fraud." Randy Alison Aussenberg, *Errors and Fraud in the Supplemental Nutrition Assistance Program (SNAP)*, Cong. Research Service, Sept. 28, 2018, at 17-18, 23, and 29.

[7] The Maryland Department of Mental Health and Hygiene uses Social Security Numbers ("SSNs") to, among other things, to maintain databases under the CDC's National Breast and Cervical Cancer Early Detection Program ("NBCCEDP"). Among other things, SSNs are used for this database to decline state funding for cancer screening if they are Medicaid ineligible. "The electronic claims administration system (eCMS) runs every claim file against the MA eligibility file and rejects claims for Program patients found [Medicaid ineligible]." *Letter from James P. Johnson, Deputy Secretary of Operations, Maryland Department of Health and Mental Hygiene, to Sen. Delores G. Kelley and Del. Susan C. Lee, Aug. 21, 2007.*

[8] 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).

- Is directed to prevent terrorist attempts to access the American financial services system[9] and hard targets.[10]

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." 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."[11]

The Fair Credit Reporting Act and the Definition of "Consumer Report"

The FCRA regulates consumer reports. The nuanced components of the definition matter because CRAs have access to a variety of information in addition to that which constitutes a "consumer report," including credit header information 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 then
- 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.[12]

Regulators and courts are clear: Since credit header information does not bear on one of the seven § 603(d)(1) factors and 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

---

[9] Federal investigators hunting for potential terrorists have been poring over hundreds of fraudulent Social Security numbers generated by a Southern California ring that catered mostly to Middle Eastern immigrants. Three people have pleaded guilty in the scheme, broken up before the Sept. 11 attacks, including a Jordanian national who worked in security at Los Angeles International Airport and a U.S. government employee who tapped a secure federal computer to procure the government-issued cards, court records and interviews show. 'Obviously,' one law enforcement official said, '[we need] to make sure no terrorists are running around with … identities that are not theirs.' Rich Connell, Greg Krikorian, *Agents Tracking Fake Social Security Cards Probe: Terrorist attacks prompt scrutiny of those who bought numbers from Southland ring*, Los Angeles Times, April 4, 2002.

[10] "At least seven of the hijackers also obtained Virginia state ID cards, which would serve as identification to board a plane, even though they lived in Maryland motels. 'If we can't be sure when interacting that someone is who they purport to be, where are we?' said James G. Huse Jr., the Social Security Administration's inspector general." Source: Robert O'Harrow Jr. and Jonathan Krim, *National ID Card Gaining Support,* Washington Post, Dec. 7, 2001, A1 (quoting James Huse, Inspector General of the Social Security Administration).

[11] 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/.

[12] *See gen. FCRA Section* 604(d)(1).

support a different interpretation and the CFPB should not take action to overturn well-settled precedents by fiat.

It would be a gross misuse of the Advisory Opinions Policy ("AOP") for the CFPB to issue an opinion that completely contradicts settled law. The AOP is designed to clarify, not rewrite, the law:

> The Bureau will focus primarily on clarifying ambiguities in its regulations, although Advisory Opinions may clarify statutory ambiguities. The Bureau will not issue advisory opinions on issues that require, or are better addressed through, a legislative rulemaking under the APA. For example, the Bureau does not intend to issue an advisory opinion that would change regulation text or commentary.

85 Fed. Reg. 77987 (Dec. 3, 2020). The AOP must not be used as a vehicle for propagating what is tantamount to one-sided informal rulemaking, particularly one that is antithetical to well-settled law.

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.[13] 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.[14] 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."[15] Further, "[t]he data at issue here reflects biographical information generally recognized as header data and, thus, **is not a consumer report**."[16] The Sixth Circuit made a similar pronouncement in *Bickley v. Dish Network, LLC*, stating that "header information" is not a consumer report.[17] Multitudes of other federal courts have stated the same.[18]

---

[13] No. 2:15-CV-14365, 2017 WL 4003437, at *3 (E.D. Mich. Sept. 12, 2017).
[14] *Id.* at *2.
[15] *Id.* at *3 (emphasis added).
[16] *Id.* (emphasis added).
[17] 751 F.3d 724, 729 (6th Cir. 2014).
[18] *See, e.g.*, *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

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.[19] 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.[20] 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."[21] 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 addresses(es)." This exclusion reinforces the position that such information is not regulated by the FCRA.[22]

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" products or services for identity authentication or fraud or identity theft detection, prevention, or investigation, signaling that identity verification products are not covered by the FCRA.[23] 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."[24]

---

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.").

[19] *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").

[20] *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.

[21] *See* 65 Fed. Reg. 33645, 33668 (May 24, 2000) (noting that age, which may be included in credit header, may be considered consumer report information).

[22] *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-0118_consumer-reports-what-information-furnishers-need-to-know_2018.pdf.

[23] 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.

[24] "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.

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

The consumer groups' letter implies that if the CFPB does not act to govern credit header information under the FCRA, such information and its use are left unprotected and unregulated. That assertion is incorrect. The GLBA strictly regulates the use and disclosure of credit header information from financial institutions. Fair, accurate, and appropriate use of credit header information is necessary to protect consumers and is well-established in law.

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

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

Extending FCRA requirements to credit header information contradicts over 50 years of law and policy. Such extension would also unnecessarily restrict the beneficial uses of such 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.

The use of non-FCRA credit header information is essential to many services. In one of many examples, CDIA members offer fraud prevention and detection services to prevent fraud on businesses, consumers, and third parties. Fraud prevention and detection 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. However, 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.

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. Further, small businesses 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.

Restricting the sharing of credit header data to only those permissible purposes under the FCRA would eliminate the ability of fraud prevention companies and users of those services to detect and defend against fraud patterns, including synthetic identity fraud. For example, detecting fraud patterns requires the analysis of a network of information across multiple identities and sources of information. Limiting the analysis to only the credit header information in a particular consumer's file inherently limits the ability to detect potential patterns and associations indicative of fraud, such as multiple identities connected to the same address.

To benefit consumers, to help prevent fraud, 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. Instead, CDIA encourages the CFPB to educate consumers on what constitutes credit header information, how it is used and disclosed, and the benefits of such uses to consumers and businesses alike. Such educational efforts better serve the CFPB's mission to "make consumer financial markets work for consumers, responsible providers, and the economy as a whole."[25]

Sincerely,

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

[25] "The Bureau," CFPB, available at https://www.consumerfinance.gov/about-us/the-bureau/#:~:text=We%20protect%20consumers%20from%20unfair,to%20make%20smart%20financial%20decisions.