epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

☎ +1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CONSUMER FINANCIAL PROTECTION BUREAU

On the Small Business Advisory Review Panel for Consumer Reporting Rulemaking

October 30, 2023

I. Introduction

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Consumer Financial Protection Bureau (CFPB or the Bureau)'s Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration (Outline), published on September 15, 2023.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has long advocated for privacy rights and robust safeguards to protect consumers. As EPIC has detailed in previous comments, data brokers frequently engage in exploitative data collection, retention, and sharing practices and enable other harmful uses of personal data.[3] EPIC has called on regulators to rein in the abusive practices of brokers, including through the use of data minimization rules under which personal data can only be collected, used, or disclosed as necessary

[1] Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration, Consumer Financial Protection Bureau (Sept. 15, 2023) [hereinafter "SBREFA Outline"].
[2] *About Us*, EPIC, https://epic.org/about/ (2023).
[3] EPIC, Comments on CFPB Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16,951 (Jul. 14, 2023) [hereinafter "July Data Broker Comments"].

to fulfill purposes consistent with reasonable expectations of consumers.[4] EPIC has also fought for greater transparency and oversight into how companies collect, use, and disseminate personal data[5] and stricter enforcement to safeguard the rights of consumers.[6]

EPIC supports the CFPB's efforts to regulate the collection and dissemination of personal information through rulemaking. EPIC has previously engaged with the Bureau's work on this issue through our January 2023 comments on the CFPB's Rulemaking on Personal Financial Data Rights,[7] our February 2023 coalition letter regarding credit header data,[8] and our July 2023 comments in response to the Bureau's Request for Information regarding data brokers.[9] We commend the Bureau for proposing rules which will strengthen protections for consumers. With this comment, we recommend refinements to the CFPB's proposals and identify additional provisions the Bureau should include in its final rule.

II. EPIC Supports the CFPB's Proposals Under Consideration

As the Bureau highlights in its Outline, the Fair Credit Reporting Act (FCRA) provides important regulatory guardrails that protect consumers from harm in the consumer reporting

[4] *See, e.g.*, Consumer Reps. & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

[5] *See, e.g.*, Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors: Hearing Before the H. Comm. on House Admin., 117th Cong. 53 (2022), https://epic.org/documents/hearing-on-big-data-privacy-risks-and-needed-reforms-in-the-public-and-private-sectors/ (statement of Caitriona Fitzgerald, Deputy Director, EPIC); EPIC, Comments on CFPB Inquiry into Big Tech Payment Platforms, 86 Fed. Reg. 61,182 (Dec. 21, 2021), https://epic.org/documents/epic-comments-on-cfpb-inquiry-into-big-tech-payment-platforms/.

[6] *See, e.g.*, EPIC, Comments on CFPB Request for Information on the Equal Credit Opportunity Act and Regulation B, 85 Fed. Reg. 46600 (Oct. 2, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CFPB-Oct2020-AI-ML.pdf.

[7] EPIC, Comments on CFPB on the Consumer Financial Data Rights Rulemaking (Jan. 25, 2023) [hereinafter "January Financial Data Rights Comments"].

[8] Coalition Letter to CFPB Requesting Broad Consumer Financial Market Correction, Beginning with an Advisory Opinion Regarding Credit Header Data (Feb. 8, 2023), https://epic.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf [hereinafter "Credit Header Letter"].

[9] July Data Broker Comments.

industry. However, the CFPB must promulgate rules pursuant to its FCRA authority to ensure that individuals continue to be protected from harms caused by consumer reporting agencies—including data brokers—given dramatic changes in technology and the state of the market.

Today, data brokers construct deeply revealing dossiers of individuals' personal information, both in terms of the breadth of data points included and the sensitive nature of much of that data.[10] In addition to selling consumer data to other public and private entities,[11] data brokers also use personal information to develop assessment tools, risk scores, and inferences, which they market as tools to help companies make decisions.[12] The same data is used to inform targeted advertising and influence consumer behavior, and consumers have little control over how their own identities are commodified.[13] Despite the harms caused by the personal data industry, consumers often lack awareness of how their data is collected, used, and disseminated—not to mention any control over their own data.[14]

[10] Staff of S. Comm. on Com., Sci., & Transp., A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes at ii (Dec. 18, 2013), https://www.commerce.senate.gov/services/files/0D2B3642-6221-4888-A631-08F2F255B577.

[11] *See, e.g.*, Matt O'Brien & Frank Bajak, *Priest Outed Via Grindr App Highlights Rampant Data Tracking*, Associated Press (July 22, 2021), https://apnews.com/article/technology-europe-business-religion-data-privacy97334ed1aca5bd363263c92f6de2caa2.; Joseph Cox, *Data Broker is Selling Location Data of People Who Visit Abortion Clinics*, Vice (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood; Memorandum from Chino Police Detective Jason Larkin on the Chino Police Contract with Fog Data Science 25 (Oct. 10, 2019), https://www.documentcloud.org/documents/22187494-chino_2019-20_attachments#document/p25/a2143086.

[12] *See, e.g.*, *CLEAR Risk Inform*, Thomson Reuters (last visited July 10, 2023), https://legal.thomsonreuters.com/en/products/clear-risk-inform; *Credit Risk Assessment and Management*, LexisNexis Risk Solutions (last visited July 10, 2023), https://risk.lexisnexis.com/corporations-and-non-profits/credit-risk-assessment. For more on the impact of data-broker risk scoring offerings, see, e.g., Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 8–17 (2014).

[13] *See* Urbano Reviglio, *The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview*, 11 Internet Pol'y Rev. 1, 2 (2022).

[14] *Id.*, EPIC, Comments on FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 34, 87 Fed. Reg. 51273 (Nov. 21, 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter "EPIC Commercial Surveillance FTC Comments"].

We commend the Bureau for considering rules which will provide the stronger protections consumers need against exploitative data broker and consumer reporting practices. In this section, we recommend further refinements related to (i) FCRA coverage of data brokers, (ii) credit header data, (iii) targeted marketing, and (iv) data security protections.

i. Expanding FCRA Coverage Over Data Brokers

This section is responsive to Questions 8 and 10.

As we explained in our July comments in response to the Bureau's Request for Information Regarding Data Brokers, data brokers should be viewed as consumer reporting agencies (CRAs) under the FCRA.[15] The CFPB's current proposals would expand FCRA coverage over data brokers by codifying a broader definition of "consumer reports," specifying that data brokers which sell certain categories of consumer data are CRAs and that data brokers which collect consumer information for permissible purposes under the FCRA may not sell the information for impermissible purposes. The Bureau cites concerns that some data brokers which engage in very similar activities to traditional credit reporting agencies (CRAs) or sell the same types of data as CRAs are not covered by the FCRA currently.[16] For example, Thomson Reuters is a data broker that markets algorithmic and automated risk analytic products to healthcare, unemployment, and social services entities in the United States.[17] The company claims that it is not a CRA under the FCRA.[18] However, its Fraud Detect system, formerly known as FraudCaster, incorporates consumer report data to generate fraud risk scores.[19] Thomson Reuters offers—through either direct contracts or

[15] July Data Broker Comments at 51.
[16] SBREFA Outline.
[17] *See Improve Fraud Detection and Prevention with Fraud Detect*, Thomson Reuters, https://legal.thomsonreuters.com/en/products/fraud-detect (last visited Oct. 3, 2023); Contract Between Il. Dep't of Emp. Sec. and Pondera Solutions 4, https://perma.cc/NQ8M-9QPA.
[18] *FCRA Notice*, Thomson Reuters, https://www.thomsonreuters.com/en/products-services/government.html (last visited Oct. 30, 2023).
[19] *See* D.C. Dep't of Hum. Servs., Pondera Proposal 3, 7–8 (2020), https://perma.cc/9SCU-GSFW; D.C. Dep't of Hum. Servs., Pondera Master Design Document 5-6, 10 (2021), https://perma.cc/28C6-2NJF.

cooperative purchasing agreements—its Fraud Detect system to the governments of 42 states, the District of Columbia, and Guam.[20] The company claims that Fraud Detect prevents public benefits fraud by analyzing data about benefits recipients.[21] Despite claiming not to be a CRA, Thomson Reuters provides an analytics tool that uses consumer report data to generate fraud alerts and similar determinations of consumers' creditworthiness, character, general reputation, and personal characteristics.[22] The CFPB should clarify that data brokers are presumptively CRAs to prevent data brokers from avoiding responsibilities they rightly bear under the FCRA.

The CFPB proposes to expand and clarify FCRA coverage over data brokers, which will provide important protections for consumers. However, we urge the Bureau to clarify that all data brokers are presumptively CRAs in the rule. As the CFPB makes clear in the SBREFA outline, the scope of the FCRA is very broad, and entities need not always use the information they collect to furnish consumer reports to be considered a CRA. An entity that furnishes information for consumer reports 10% of the time—or even just expects to furnish consumer reports—meets the threshold to qualify the data as a consumer report.[23] The information data brokers collect and disseminate generally fulfills the definition of a consumer report, so the entities should presumptively be considered CRAs. The FCRA defines a consumer report, with some exceptions, as a communication by a CRA "bearing on a consumer's credit worthiness, credit standing, credit capacity, character,

[20] *See* Grant Fergusson, EPIC, Outsourced and Automated: How AI Companies Have Taken Over Government Decision-Making 14, 39 (2023), https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf.

[21] *Id*. at 14.

[22] *See* 15 U.S.C. § 1681a(d).

[23] *See* NCLC FCR § 2.3.5.3 45; NCLC FCR § 2.3.1.2 33 n.35 (citing *Miller v. Trans Union*, 2013 WL 5442008 (M.D. Pa. Aug. 14, 2013) (actual transmission of report to third party is not necessary for it to be a consumer report, so long as it is expected to be used or collected for purposes of transmission), adopted in part, 2013 WL 5442059 (M.D. Pa. Sept. 27, 2013)). *Cf. Coulter v. Chase Bank*, 2020 WL 5820700, at *11 (E.D. Pa. Sept. 30, 2020) (summary judgment denied where defendant failed to provide authority for proposition that information appearing on consumer disclosure and alleged to ultimately impact consumer's report and score is not actionable under the FCRA).

general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility" for enumerated purposes such as credit, insurance, underwriting, and employment.[24] This broad definition of consumer report goes far beyond traditional credit reports. Whether records contain inferences can bear significantly on whether a record is a consumer report, but even datasets containing only names and addresses may constitute a consumer report if the record is used to make eligibility determinations.[25] Data brokers often market inference, risk assessment, and algorithmic scoring tools built using consumer report data, and the tools are used to make eligibility determinations.[26] Because data brokers are in the business of aggregating and selling consumer reports, they should be considered CRAs under FCRA.

The core business model of the data broker industry requires sharing third-party data, which may be combined with first-party data collected by the broker. When data brokers combine first-party data with any third-party data which is subject to the FCRA, the entire dataset should be subject to the FCRA because it includes FCRA-covered data.[27] Given the breadth of data collected, stored, and disseminated by data brokers, the likelihood that data brokers share FCRA-covered data is so high that data brokers should be presumed to be CRAs unless they can demonstrate that they continuously undertake reasonable measures to prevent the data they collect and disclose from being

[24] 15 U.S.C. § 1681a(d)(1).

[25] *See* 2011 FTC Staff Summary § 603(d)(1) Item 6(C)(ii) ("A list of consumers' names and addresses, if assembled or defined by reference to characteristics or other information that is also used (even in part) in eligibility decisions, is a series of consumer reports. For example, a list comprised solely of consumer names and addresses, but compiled based on the criterion that every name on the list has at least one active trade line, updated within six months, is a series of consumer reports.").

[26] *See, e.g.*, *CLEAR Risk Inform*, Thomson Reuters (last visited July 10, 2023), https://legal.thomsonreuters.com/en/products/clear-investigation-software/clear-risk-inform; *Credit Risk Assessment and Management*, LexisNexis Risk Solutions (last visited Oct. 30, 2023), https://risk.lexisnexis.com/corporations-and-non-profits/credit-risk-assessment. For more on the impact of data-broker risk scoring offerings, see, e.g., Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 8–17 (2014).

[27] July Data Broker Comments at 51.

used for any of the FCRA's enumerated purposes. Further, the CFPB should clarify that data brokers may not avoid FCRA coverage if those ostensibly reasonable measures prove insufficient in fact.

The FCRA imposes important requirements on CRAs pertaining to data collection, sales, and retention for the purpose of creating and disclosing consumer reports. Extending FCRA coverage to data brokers would mitigate many of the consumer privacy harms that the data broker industry causes. In our July comments, we highlighted the risk of downstream misuse of data shared by data brokers. Even if data brokers disseminate seemingly innocuous data points about consumers, that data could later be combined with other information to identify individuals without their consent,[28] used to make inaccurate inferences about consumers,[29] and used to train and maintain harmful automated decision-making systems.[30] Presumptively classifying data brokers as CRAs would help to protect consumers from downstream misuse of their data by entities who buy and sell consumer information from data brokers.

ii. Credit Header Data

This section is responsive to Question 18.

In February, EPIC and a coalition of peer organizations wrote to the CFPB urging the Bureau to clarify that credit header data satisfies the definition of a consumer report when it is derived from

[28] *See* Sara Geoghegan & Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC Blog (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/; Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data that Tracked Gay Priests*, Wash. Post (Mar. 9, 2023), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/.

[29] *See, e.g.,* EPIC, Screened & Scored in the District of Columbia 23 (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf; *see also* Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1257 (2020); Devin G. Pope & Justin R. Sydnor, *Implementing Anti-Discrimination Policies in Statistical Profiling Models*, 3 A. Econ. J. 206, 209 (2011); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2 Colum. Bus. L. Rev. 494 (2019).

[30] *See* EPIC Commercial Surveillance FTC Comments at 86; Kevin Schaul et al., *Inside the Secret List of Websites that Make AI Like ChatGPT Sound Smart*, Wash. Post (Apr. 19, 2023), https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/; Ari Ezra Waldman, *Power, Process and Automated Decision-Making*, 88 Fordham L. Rev. 613, 615–16 (2019).

data originating from a CRA and is data that is typically included in consumer reports issues by CRAs.[31] Credit header data usually includes data such as an individual's name, aliases, birth date, Social Security number, current and prior addresses, and telephone number.[32] Consumer information, including credit header data, should always be classified as a consumer report when it originates from a CRA and the information otherwise fulfills the definition of a consumer report.[33] Credit header data is derived from CRA files and otherwise users in consumer reports, so it is a consumer report under the FCRA.[34]

We commend the Bureau for considering a proposal to clarify the extent to which credit header data constitutes a consumer report. As we set out in our coalition letter, we urge the Bureau to adopt a rule clarifying that there is no categorical exception for credit header information and reiterating that credit header information satisfies the statutory consumer report definition when it is derived from data originating from a CRA and is otherwise included in consumer reports issued by the CRA. The rule should further clarify that consumer information from a CRA, regardless of content, is always a consumer report.[35]

iii. Targeted Marketing

This section is responsive to Questions 19 and 20.

As the SBREFA outline makes clear, providing consumer reports to third parties for marketing and advertising is not a permissible purpose under the FCRA, so CRAs must not furnish consumer reports for this purpose.[36] However, as the outline also discusses, CRAs often work with third parties to combine consumer reports with third-party data and then deliver marketing and

[31] Credit Header Letter.
[32] FTC, Individual Reference Services-A Report to Congress (1997), https://www.ftc.gov/reports/individual-reference-services-report-congress.
[33] 15 U.S.C. § 1681a(d)(1).
[34] Credit Header Letter
[35] *Id*.
[36] *See* 15 U.S.C. 1681b(c).

advertising materials on behalf of the third party. Though CRAs in this instance do not transfer the consumer reports to the third parties, they permit third parties to utilize the consumer reports for advertising purposes without consumer consent—and without a permissible purpose.[37] The CFPB should clarify in its rule that such uses of consumer reports to deliver marketing materials on behalf of third parties is a violation of the FCRA.

This section is responsive to Question 21.

The FCRA covers consumer data that can reasonably be linked to an individual. The Bureau should clarify that this category includes aggregated or nominally "anonymized" data that can still be linked to an individual, as well as data that can combined with other data and used to reidentify an individual. For example, data pertaining to a neighborhood may not be covered by the FCRA because it may not be possible to link the data to an individual, but household- or device-level data is reasonably linkable to individuals; the rule should clarify that this data is covered by the FCRA.[38] Whenever aggregated or "anonymized" data is combined with other data to reidentify individuals, both the original dataset and the resulting dataset should then be covered by the FCRA.

iv. Data Security Protections

This section is responsive to Question 4.

We commend the CFPB for considering proposals to address CRAs' obligations under the FCRA to protect consumers from data breaches. The FCRA must meet modern data security challenges, especially given the massive risk of harm to consumers posed by breaches of personal information. We encourage the Bureau to include specific data security measures in its rule, and we provide the following non-exhaustive list of provisions that the Bureau should adopt.

[37] July Data Broker Comments at 68-71.

[38] *Id*. at 74–75; *See* 2011 FTC Staff Summary at 11 ("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'").

First, we urge the Bureau to require CRAs to implement reasonable data security practices to protect consumer data. The rule should consider a data security procedure to be *per se* unreasonable under the FCRA if the procedure ultimately results in an unauthenticated disclosure.[39]

Second, the rule should incorporate principles of data minimization.[40] The rule should update the definition of "abandoned" files in 16 C.F.R. § 682 to include digitally stored files which are "no longer strictly necessary for business purposes." The rule should provide a uniform standard for deletion of consumer records that are no longer necessary to provide the service the customer requested, and CRAs should also be required to delete consumer records upon request by consumers.[41]

Third, the rule should clearly state that creating consumer accounts without consent is impermissible, and the rule should clearly define how CRAs may gain consent from consumers without manipulation or coercion.[42]

Fourth, the rule should clarify that when CRAs use data clean rooms, in which data assets are intermingled "for specific, mutually agreed upon uses, while guaranteeing enforcement of strict data access limitations,"[43] the CRAs and other entities involved in the clean room mechanism must comply with the FCRA if any of the data enriched in the clean room mechanism is covered by the FCRA.[44] When data that is covered by the FCRA is covered by non-covered data, the combined dataset is then subject to the FCRA. Entities use clean rooms to combine and compare data, and they will do so even more with the deprecation of third-party cookies and increasing use of consumer

[39] July Data Broker Comments at 61-63.
[40] 16 C.F.R. § 682.1(c)(1).
[41] January Financial Data Rights Comments at 6.
[42] July Data Broker Comments at 58.
[43] IAB Tech Lab, *Data Clean Rooms: Guidance and Recommended Practices Version 1.0*, 10 (July 5, 2023), https://iabtechlab.com/blog/wp-content/uploads/2023/06/Data-Clean-Room-Guidance_Version_1.054.pdf; *see also* Jon Keegan, *What Are "Data Clean Rooms"?*, Markup (July 1, 2023), https://themarkup.org/hello-world/2023/07/01/what-are-data-clean-rooms.
[44] *Id*. at 54–55.

privacy tools.[45] The CFPB should make clear that datasets containing consumer reports are covered by the FCRA when entities use data clean room mechanisms to process the datasets.

Finally, we recommend the CFPB to include similar data security requirements to the requirements of the Federal Trade Commission's Safeguards Rule, which took effect in June. Those standards include access controls, secure password practices, user authentication, system segmentation, traffic monitoring, staying current on known vulnerabilities, security reviews, and employee training.[46] The FTC has also recently amended the Safeguards Rule to require entities to report certain data breaches to the FTC as soon as possible, and no later than 30 days, after the discovery of a security breach affecting at least 500 customers.[47] We recommend that the CFPB incorporate similar data breach notification requirements into the rule.

III. EPIC Recommends Several Additions to the Rule

This section is responsive to Question 4.

In our previous comments to the CFPB, we recommended that the Bureau incorporate the following provisions into a rule: (i) know your customer protocols, (ii) protections for the use of alternative data in credit scoring models, (iii) a ban the use of credit scoring in tenant screening and public benefits determinations, and (iv) a ban on the use of pre-conviction criminal proceeding information in credit reports. These provisions would help to protect consumers from harms caused

[45] *See, e.g.*, Pamela Parker, *What is Identity Resolution and How are Platforms Adapting to Privacy Changes?*, MarTech (June 1, 2022), https://martech.org/what-is-identity-resolution-and-how-are-platforms-adapting-to-privacy-changes/ (noting that the number of devices connected to IP networks, such as connected speakers, home management solutions, smart TVs, and wearable devices, is expected to more than triple the global population in 2023, citing to Cisco Annual Internet Report, 2018-2023). We note that DCRs is just one method of identity-stitching. Others include (but are not limited to) hashed email, publisher cohorts, universal IDs, and FLOCs. *See, e.g.*, Lore Leitner et al., *Ad Tech: How to Manage Compliance in a New First Party (or NO) Cookie World*, Priv. & Sec. Acad. (Mar. 24, 2022), https://www.privacysecurityacademy.com/ad-tech-how-to-manage-compliance-in-a-new-first-party-or-no-cookie-world/.

[46] 16 C.F.R. 314.4; January Financial Data Rights Comments at 17–18.

[47] *See FTC Updates Safeguards Rule to Require Data Breach Reporting, Adopts EPIC Recommendations*, EPIC (Oct. 27, 2023) https://epic.org/ftc-updates-safeguards-rule-to-require-data-breach-reporting-adopts-epic-recommendations/.

by misuse of consumer data, limit discrimination in credit scoring, and promote accuracy in consumer reporting. We again urge the CFPB to include these provisions in its rule.

i. Know-Your-Customer Protocols

As discussed in section II.i of this comment, downstream misuse of consumer data poses risks to consumers. These risks include the possibility that previously anonymized data can be reidentified and used for harmful purposes, data breach risks, and risks that data will be used to train and deploy harmful algorithmic decision-making tools. We recommend that the rule require data brokers to use know-your-customer (KYC) protocols to mitigate downstream misuse of data.[48] This would require CRAs to undertake ongoing monitoring of users of consumer reports, which builds on existing FCRA due diligence requirements.[49]

ii. Protections for the Use of Alternative Data in Credit Scoring Models

When proposing a rule to better protect individuals from data brokers and consumer reporting agencies, the Bureau must consider persons without credit scores and those who rely on alternative data to obtain credit. Notably, the FTC has pursued FCRA enforcement against entities that utilize alternative data in credit scoring models,[50] and the Commission has noted that data not traditionally associated with creditworthiness (e.g., ZIP code, social media usage, shopping history, name capitalization) is subject to the FCRA if the alternative data is used to evaluate a consumer's eligibility for credit, employment, insurance, housing, or other benefits and transactions.[51] The rule

[48] July Data Broker Comments at 59.

[49] *See* NCLC FCR § 7.5.2.2 474 (citing 2011 FTC Staff Summary § 607(a) Item 4B); 2011 FTC Staff Summary § 607(a) Item 3.

[50] *See, e.g*., Press Release, FTC, 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.

[51] *See, e.g*., FTC, *Big Data: A Tool for Inclusion or Exclusion?* at ii (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

should clarify that alternative data collected from secondary sources used to determine a consumer's risk level is a consumer report if the data is disseminated to a third party.[52]

iii. Ban the Use of Credit Reports in Tenant Screening Determinations

We urge the CFPB to ban the use of credit reports in tenant screening in its rule.[53] Credit reports often contain errors, are not up to date, and do not reflect a consumer's current ability to pay.[54] Further, using a credit report to determine eligibility for tenancy perpetuates housing inequality and economic injustice.

For further information regarding the need to prohibit the use of credit reports in tenant screening, we recommend the Bureau refer to the National Consumer Law Center's resource on this topic, *2023 Consumer Reform Priorities to Protect Tenants*.

iv. Ban the Use of Pre-Conviction Criminal Proceeding Information in Credit Reports

Similar to using credit reports in tenant screening, utilizing pre-conviction criminal proceeding information such as arrest records in credit reporting also introduces inaccuracy and perpetuates inequality.[55] Before someone has been convicted of a crime, no determination of guilt or innocence has been made, so that person's involvement in the proceeding should have no bearing on

[52] July Data Broker Comments at 66.

[53] *Id*. *See generally* Chi Chi Wu, *Even the Catch-22s Come With Catch-22s: Potential Harms & Drawbacks of Rent Reporting*, NCLC (Oct. 24, 2022), https://www.nclc.org/resources/even-the-catch-22s-come-with-catch-22s-potential-harms-drawbacks-of-rent-reporting/ (rent payment data is new trove of info but it will be used at expense of vulnerable renters); NCLC, Comments on Tenant Screening Request for Information by FTC and CFPB (May 30, 2023), https://www.nclc.org/resources/comments-on-tenant-screening-request-for-information-by-ftc-and-cfpb/; Chi Chi Wu & Michael Best, *Why We Need the Fair Chance in Housing Act (FCHA) to Keep Credit Reports Out of Housing Decisions Now*, NCLC (Mar. 15, 2023), https://www.nclc.org/resources/why-we-need-the-fair-chance-inhousing/.

[54] *See, e.g.*, NCLC, *Fact Sheet, An Act Relative to the Use of Credit Reporting in Housing H1429/S894, the Fair Chance in Housing Act: Senator Lesser, Representative Malia*, https://www.nclc.org/wp-content/uploads/2022/09/MA_Credit_Housing.pdf (last visited Oct. 30, 2023); EPIC, Screened & Scored in the District of Columbia 8, 13, 24-25, 29 (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf.

[55] July Data Broker Comments at 67.

their creditworthiness or eligibility for other benefits.[56] Evidence shows that arrest statistics are influenced by racial bias, and using pre-conviction criminal proceeding data perpetuates that bias and introduces inaccuracy into credit reporting.[57] We urge the CFPB to prohibit the use of pre-conviction data in credit reports to better protect consumers.

IV. Conclusion

We commend the CFPB's work to strengthen protections for consumers in data broker and consumer reporting industries. In this comment and our previous engagements with the Bureau, we have highlighted the harms consumers experience from exploitative data collection, sharing, and use practices, improper data security protections, discriminatory uses of credit reporting data, and downstream misuse of consumer data. This rule presents an opportunity for the CFPB to update FCRA regulations to better protect consumers in the modern credit reporting ecosystem. We appreciate this opportunity to comment, and we are eager to engage with the Bureau further as the rulemaking process continues. If you have any questions, please contact EPIC Director of Litigation John Davisson (davisson@epic.org).

Respectfully Submitted,

/s/ John Davisson

John Davisson
Director of Litigation
davisson@epic.org

[56] *See, e.g.*, Aaron Rieke et al., Upturn, Open Soc'y Founds., Data Brokers in an Open Society 37 (2016), https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-inan-open-society-20161121.pdf; Rebecca Oyama, *Do Not (Re)Enter: The Rise of Criminal Background Tenant Screening as a Violation of the Fair Housing Act*, 15 Mich. J. Race & L. 181, 188 (2009).

[57] *See, e.g.*, Magnus Loftstrom et al., *Racial Disparities in Law Enforcement Stops*, Prison Pol'y Inst. Cal. (2021), https://www.ppic.org/publication/racial-disparities-in-law-enforcement-stops/; The Sentencing Project, *Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System* (2018), https://www.sentencingproject.org/reports/report-to-the-united-nations-on-racial-disparities-in-the-u-scriminal-justice-system/; U.S. Gov't Accountability Off., GGD-94-29R, Racial Differences in Arrests (1994), https://www.gao.gov/products/ggd-94-29r.

/s/ Caroline Kraczon
Caroline Kraczon
Law Fellow
kraczon@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)