COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, NATIONAL CONSUMERS LEAGUE, and CONSUMER FEDERATION OF AMERICA

to the

CONSUMER FINANCIAL PROTECTION BUREAU

On the Protecting Americans from Harmful Data Broker Practices Notice of Proposed Rulemaking

CFPB-2024-0044

April 2, 2025

I. Introduction

The Electronic Privacy Information Center (EPIC), National Consumers League, Consumer Federation of America, and the undersigned organizations submit these comments in response to the Consumer Financial Protection Bureau ("CFPB" or "the Bureau")'s proposed rules on Protecting Americans from Harmful Data Broker Practices, published on December 3, 2024.

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.[1] EPIC has long advocated for privacy rights and robust safeguards to protect consumers. As EPIC has previously detailed, data brokers frequently engage in exploitative data collection, retention, and sharing practices and enable other harmful uses of personal data.[2] 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 to fulfill

[1] *About Us*, EPIC, https://epic.org/about/ (2023).
[2] 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"]; EPIC, Comments on CFPB Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals (Oct. 30, 2023) [hereinafter "October SBREFA Comments"].

purposes consistent with reasonable expectations of consumers.[3] EPIC has also fought for greater transparency and oversight of how companies collect, use, and disseminate personal data[4] and stricter enforcement to safeguard the rights of consumers.[5]

EPIC supports the CFPB's efforts to regulate the collection and dissemination of personal information through its Fair Credit Reporting Act (FCRA) 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,[6] our February 2023 coalition letter regarding credit header data,[7] our July 2023 comments in response to the Bureau's Request for Information regarding data brokers,[8] our October 2023 comments in response to the Bureau's Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals,[9] and our August 2024 Comments on the CFPB's proposed rules on the Prohibition on Creditors and Consumer Reporting Agencies Concerning Medical Information.[10] We commend the Bureau for proposing rules which will strengthen protections for consumers.

---

[3] *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.
[4] *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/.
[5] *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.
[6] EPIC, Comments to CFPB on the Consumer Financial Data Rights Rulemaking (Jan. 25, 2023) [hereinafter "January Financial Data Rights Comments"].
[7] 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"].
[8] July Data Broker Comments.
[9] October SBREFA Comments.
[10] EPIC, Comments to CFPB on the Prohibition on Creditors and Consumer Reporting Agencies Concerning Medical Information, CFPB-2024-0023 (Aug. 13 2024), https://epic.org/documents/comments-of-epic-to-the-cfpb-on-the-prohibition-on-creditors-and-consumer-reporting-agencies-concerning-medical-information/.

The National Consumers League (NCL) is a nonprofit, nonpartisan consumer advocacy organization representing consumers and workers on marketplace and workplace issues since its founding in 1899. Headquartered in the District of Columbia, NCL provides government, businesses, and other organizations with the consumer's perspective on concerns including fraud, privacy, child labor, food safety, healthcare, and telecommunications. Since 1992, NCL has accepted thousands of consumer complaints each year through its anti-scam project, Fraud.org.

The Consumer Federation of America (CFA) is an association of over 250 non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

With this comment, we recommend refinements to the CFPB's proposals and identify additional provisions the Bureau should include in its final rule.

II. Data broker harms

The business model of data brokers is built upon mass extraction and sale of personal information. Consumers have little control or awareness as to how brokers collect, use, and sell deeply personal insights about them. Data brokers impose real harm on people by degrading privacy, security, and safety. These harms impact individuals, communities, and our country at large. This section highlights a few specific examples of harms caused by data brokers, but the range of such harms is certainly not limited to this list.

i. Privacy harms

Data brokers pose a significant threat to privacy because of the massive scope and scale of personal information they collect and sell. Data brokers construct deeply revealing dossiers of individuals' personal information, as measured by both the breadth of data points included and the

sensitive nature of much of that data.[11] Data brokers make intimate personal information available for sale on the open market, enabling bad actors to use private information to track, threaten, and inflict reputational harm on individuals.[12] In addition to selling consumer data to other public and private entities, data brokers also use personal information to develop assessment tools, risk scores, and inferences, which they market as tools to help companies make decisions.[13] 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.[14]

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 safeguards against the misuse of their own data even when they are aware.[15] Several states have passed laws requiring businesses to allow consumers to opt out of data collection and sale.[16] However, the opt-out process

---

[11] 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.

[12] *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.

[13] *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).

[14] *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).

[15] *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"].

[16] Yael Grauer, Victoria Kauffman, and Leigh Honeywell, Data Defense: Evaluating People-Search Site Removal Services, Consumer Reports (Aug. 8, 2024), https://innovation.consumerreports.org/wp-content/uploads/2024/08/Data-Defense_-Evaluating-People-Search-Site-Removal-Services-.pdf.

can be cumbersome and often ineffective. Consumers must file an opt-out request with each data broker site individually, and different sites use different opt-out processes. Even after completing an opt-out request, data brokers often fail to remove consumer data completely, or consumer data may reappear a few weeks or months later.[17] Several paid data broker removal services offer to file opt-out requests on consumers' behalf and continue monitoring to ensure that consumer data does not reappear in data brokers' records. But Consumer Reports found that these paid services are frequently ineffective at removing their customers' information from data broker records over the long term.[18]

ii. Fraud and scams

Consumers reported losing $10 billion to fraud in 2023 to the Federal Trade Commission ("FTC" or "Commission").[19] When adjusting for underreporting, the FTC estimates that overall fraud losses reached $158 billion in 2023. In that same year, the median loss reported to the FTC was $500.[20] Fraud.org's Top Ten Scams report for 2024 found median losses for certain scams have ballooned in recent years.[21] Consumers reported a median loss of $30,000 to Fraud.org for cryptocurrency investment scams. Victims also reported a median loss of $11,750 to Fraud.org for friendship and romance fraud.

Criminals use individuals' data to better inform their scam attempts. Personal information including names, age, and location can facilitate more convincing phishing messages and impersonations. Data brokers' profiling efforts and sale of contact information also enable fraudsters

[17] *Id*. at 5.
[18] *Id*. at 10.
[19] Protecting Older Consumers 2023-2024, Federal Trade Commission (Oct. 18, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf.
[20] Consumer Sentinel Network Data Book 2023, Federal Trade Commission (Feb. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf.
[21] Top Ten Scams of 2024, Fraud.org (Jan. 2025), https://nclnet.org/wp-content/uploads/2025/01/Top-Scams-of-2024.pdf.

to more easily target certain groups of people based on their personal characteristics (like military service or retirement status).

Federal law enforcement has built a record of action against data brokers for these practices. In 2015, the FTC sued data brokers for providing payday loan applicants' financial information to scammers, resulting in over $7 million in losses.[22] In 2020 and 2021, the U.S. Department of Justice brought cases against Epsilon LLC, Macromark Inc., and KBM Group for their sale of consumer data to scammers. Epsilon alone was responsible for the provision of 30 million individuals' information to fraudsters.[23] Macromark pleaded guilty to facilitating over $9.5 million in losses to senior scams.[24] KBM acknowledged that it sold consumer information to a number of mass-mailing fraud schemes that sent false "sweepstakes" and "astrology" solicitations to consumers.[25]

Related cases also highlight the insecurity of the current information environment. Even if a data broker or aggregator is not selling consumer information directly to criminals, they may place insufficient restrictions on the downstream uses of the data, creating risk for the surveilled individuals. Also, these companies' mass collection of consumer data makes them attractive targets for data breaches, a problem that has reached record levels.[26]

In 2024, the FTC charged X-Mode/Outlogic with violations of law stemming from the company's sale of precise consumer locations, the failure to sufficiently restrict the uses of that sold

[22] FTC Charges Data Brokers with Helping Scammer Take More Than $7 Million from Consumers' Accounts, Federal Trade Commission (Aug. 12, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million-consumers-accounts.
[23] Marketing Company Agrees to Pay $150 Million for Facilitating Elder Fraud Schemes, U.S. Department of Justice (Jan. 27, 2021), https://www.justice.gov/archives/opa/pr/marketing-company-agrees-pay-150-million-facilitating-elder-fraud-schemes.
[24] List Broker Pleads Guilty to Facilitating Elder Fraud Schemes, U.S. Department of Justice (Apr. 23, 2021), https://www.justice.gov/archives/opa/pr/list-broker-pleads-guilty-facilitating-elder-fraud-schemes.
[25] Justice Department Recognizes World Elder Abuse Awareness Day; Files Cases Against Marketing Company and Executives Who Knowingly Facilitated Elder Fraud, U.S. Department of Justice (Jun. 15, 2021), https://www.justice.gov/archives/opa/pr/justice-department-recognizes-world-elder-abuse-awareness-day-files-cases-against-marketing.
[26] Data Breach Chronology, PrivacyRights.org (Feb. 9, 2025), https://privacyrights.org/data-breaches.

information, and the lack of informed consumer consent.[27] The FTC's order prohibits X-Mode/Outlogic from sharing or selling sensitive location data; the company had previously ingested more than 10 billion location data points.[28] The Commission also secured a similar ban on the selling or sharing of precise location data with InMarket after the company used that information and other data types to create advertising profiles.[29]

The CFPB's proposed rule to limit harmful sharing of consumers' personal information would help to combat the nationwide fraud epidemic. Restricting the share of data for only legally permissible purposes will cut off bad actors from directly receiving consumer information. Requiring clear consent from the surveilled individuals for disclosing data to other parties will also provide greater control to consumers over who has access to their information and how the information may be used. Lastly, a Bureau rule limiting the unlawful sale of certain data would provide greater clarity to regulated entities regarding their obligations and liabilities under federal law.

iii. Harms to national security

The data broker industry is a threat to national security.[30] Data brokers compile and sell extensive profiles of information on Americans, including members of the military and government officials. These records may contain location data, financial information, information about family

[27] FTC Finalizes Order with X-Mode and Successor Outlogic Prohibiting it from Sharing or Selling Sensitive Location Data, Federal Trade Commission (Apr. 12, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-order-x-mode-successor-outlogic-prohibiting-it-sharing-or-selling-sensitive-location.
[28] FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket, Federal Trade Commission (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket.
[29] FTC Finalizes Order with InMarket Prohibiting It from Selling or Sharing Precise Location Data, Federal Trade Commission (May 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-finalizes-order-inmarket-prohibiting-it-selling-or-sharing-precise-location-data.
[30] Data Broker Threats: National Security, Electronic Privacy Information Center (May 2024), https://epic.org/wp-content/uploads/2024/05/Data-Broker-One-Pager-National-Security-2.pdf.

members, and other sensitive information.[31] For example, 2018 reporting showed that Strava, a popular fitness tracking app, operates a "global heat map" which shows where users logged Strava activities. Researchers found that Strava's global heat map could be used to identify the location of military bases and patrol routes, as well as personally identifying information, because members of the military frequently used Strava in those areas.[32] Data brokers compile sensitive information like this and offer it for sale without measures in place to ensure that the data they sell does not expose military information or other sensitive national security information.

Data brokers' largely unregulated trade of personal data, including data with national security implications, puts our country at risk. Duke University researchers found that data brokers sell profiles containing sensitive information of active-duty military members, veterans, and their families for as little as $0.12 per record.[33] Data brokers do not use sufficient security controls to prevent sensitive national security information from ending up in the wrong hands. In fact, a report by the Irish Council for Civil Liberties found that foreign adversaries can obtain sensitive information about members of the U.S. military, politicians, and other high-profile national security officials through the real-time bidding system, which data brokers use to target online advertisements.[34] Further, bad actors can use sensitive information purchased from data brokers to

[31] Prepared Remarks of CFPB Director Rohit Chopra at the White House on Data Protection and National Security, CFPB (Apr. 2, 2024), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-ofcfpb-director-rohit-chopra-at-the-white-house-on-data-protection-and-nationalsecurity/.
[32] Jeremy Hsu, The Strava Heat Map and the End of Secrets, Wired (Jan. 29, 2018), https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackersprivacy/.
[33] Justin Sherman, Hayley Barton, Aden Klein, Brady Kruse, & Anushka Srinivasan, Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security, Duke Univ. Sanford School of Public Policy (Nov. 2023), https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-ofdata-on-us-military-personnel/.
[34] EPIC and ICCL Enforce, Complaint In the Matter of Google's RTB Practices to Federal Trade Commission (Jan. 16, 2025), https://epic.org/documents/epic-iccl-enforce-complaint-in-re-googles-rtb/; Dell Cameron & Dhruv Mehrotra, Google Ad-Tech Users Can Target National Security 'Decision Makers' and People With Chronic Diseases, Wired (Feb. 20, 2025), https://www.wired.com/story/google-dv360-banned-audience-segments-national-security/; Johnny Ryan & Wolfie Christl, America's Hidden Security Crisis: How Data

carry out blackmail or facilitate phishing tactics to obtain state secrets from military and government personnel.[35] Data brokers compile and sell information without regard to how the information could be used to threaten national security, further demonstrating the need for rules governing what information data brokers collect and when they can disclose the information to third parties.

iv. Harms to survivors of domestic violence

Data brokers enable abusers to harm domestic violence survivors by making personal information more accessible.[36] Data brokers collect and sell personal information largely without restriction and without individuals' knowledge or consent. This data includes personal identifiers like name and Social Security information, and it also includes information that could be used to find someone, including addresses, purchase history, and other location data. Data brokers frequently compile information from public records, including property records, court testimonies, and consumer data.[37] Even when survivors try to conceal their identity and location by changing their name or participating in a state address confidentiality program, data brokers sell such extensive personal information that abusers can often use it to find out a survivor's new name and address.[38] By selling so much personal information, data brokers inadvertently provide abusers with tools to locate or stalk their victims, creating serious safety threats.[39]

About United States Defence Personnel and Political Leaders Flows to Foreign States and Non-State Actors (Irish Council for Civil Liberties eds. Nov. 2023), https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-securitycrisis.pdf.

[35] Prepared Remarks of CFPB Director Rohit Chopra at the White House on Data Protection and National Security, CFPB (Apr. 2, 2024), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-ofcfpb-director-rohit-chopra-at-the-white-house-on-data-protection-and-nationalsecurity/.

[36] Data Broker Harms: Domestic Violence Survivors, Electronic Privacy Information Center & National Network to End Domestic Violence (Nov. 2024), https://epic.org/wp-content/uploads/2024/11/Data-Broker-Harms-One-Pager-Domestic-Violence-Survivors.pdf.

[37] Data Brokers: What They Are and What You Can Do About Them, National Network to End Domestic Violence (2022), https://www.techsafety.org/data-brokers.

[38] *Id*.

[39] Justin Sherman, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, Lawfare (Oct. 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-andpublicly-available-information-carve-outs.

Beyond exacerbating physical safety risks, data brokers also have a psychological impact on survivors, who experience anxiety and fear that their abusers may find them using information sold by data brokers. Survivors may also go to great lengths to avoid being included in any public records. For example, survivors may avoid renting or purchasing a new home to prevent their new address from being included in public property records that can be amplified by data brokers. Instead, survivors often resort to more unstable living arrangements like couch surfing, temporary housing, or even homelessness.[40] Survivors may also face employment instability because completing a background check at a new job can link a survivor's identity to past records, exposing survivors who have changed their names.[41] Data brokers may also compile employment information from data breaches, which can expose survivors' personal information.[42] Further, survivors may choose not to seek legal or social services that require sharing personal information because public court records are often collected and sold by data brokers.[43]

Survivors seeking justice or trying to start fresh with a new home or job are often unable to do so because the data broker industry keeps survivors in constant fear that their abuser may be able to purchase personal information that could be used to find them. Placing reasonable limits on when data brokers may disclose or sell information would help to keep vulnerable populations like domestic violence survivors safe.

[40] Why Privacy and Confidentiality Matters for Victims of Domestic & Sexual Violence, Safety Net Project (2016), https://www.techsafety.org/privacymatters.
[41] *Id.*
[42] Catherine Fitzpatrick, For domestic violence victim-survivors, a data or privacy breach can be extraordinarily dangerous, Tech Xplore (Dec. 4, 2023), https://techxplore.com/news/2023-12-domestic-violence-victim-survivors-privacybreach.html.
[43] Why Privacy and Confidentiality Matters for Victims of Domestic & Sexual Violence, Safety Net Project (2016), https://www.techsafety.org/privacymatters.

v. Harms to immigrants

Data brokers also exacerbate discrimination against immigrant populations.[44] Sensitive information such as immigration status and employment history are included in the profiles that data brokers compile and sell. Employers, landlords, and financial information can use information from data brokers to discriminate against immigrants by illegally denying them jobs, housing, or credit.[45] Landlords may also use information from data brokers to discriminate against immigrants by charging them higher rent or requiring them to have a co-signer only because of their immigration status. Financial institutions often consider immigration status when evaluating applicants for credit, and some institutions have denied credit to people simply because of their immigration status.[46]

Data brokers also enable immigration enforcement agencies to circumvent due process. Instead of following legal and constitutional processes to obtain information, Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) purchase extensive personal information from data brokers about immigrant communities.[47] These agencies use location data and home addresses purchased from data brokers to track individuals, and they also purchase access to tools that track jail bookings of undocumented immigrants. Doing so enables the agencies to detain immigrants when they are released from local custody, even when there are local prohibitions on sharing this information with federal agencies.[48] Data brokers enable extensive surveillance of

---

[44] How Data Brokers Harm Immigrants, Electronic Privacy Information Center & Just Futures Law (Oct. 2024), https://epic.org/wp-content/uploads/2024/10/Data-Broker-Harms-to-Immigrants-One-Pager-1.pdf.
45 A Place to Call Home: Housing Challenges Among Immigrant Families, National Council on Family Relations (Jun. 24, 2020), https://www.ncfr.org/ncfr-report/summer-2020/place-call-home-housing-challenges-among-immigrant-families.
[46] Sonia Lin, Protecting immigrant access to fair credit opportunities, Consumer Financial Protection Bureau (Oct. 12, 2023 https://www.consumerfinance.gov/about-us/blog/protecting-immigrant-access-to-fair-credit-opportunities/.
[47] Fighting Back Data Brokers, Just Futures Law, https://www.justfutureslaw.org/fighting-data-brokers (last visited Feb. 18, 2024).
[48] The Data Broker Loophole is Being Exploited to Target Immigrant Communities, National Association of Criminal Defense Lawyers (May 22, 2024), https://www.nacdl.org/getattachment/567b4c71-b702-47d7-a59c-1e42f39b065a/immigration-and-data-purchases.pdf.

immigrant populations, both by private entities and the government, resulting in discrimination and denial of due process.

vi. Harms to public officials

In recent years, violence targeting public officials, including law enforcement officers and judges, has been on the rise.[49] People who wish to harm public officials can use personal information purchased from data brokers to locate and track their victims. For example, in July 2020, Daniel Anderl, the son of U.S. District Court Judge Esther Salas, was murdered at the family's home. The gunman, seeking to harm Judge Salas, posed as a deliveryman and shot Daniel when he answered the front door. The public availability of personal information online, including the judge's residential address, enabled the gunman to find her family and kill her son.[50]

Judge Salas advocated for New Jersey's passage of Daniel's Law[51], which prohibits the disclosure of certain personal information about judges, law enforcement officers, judicial officers, prosecutors, and their family members. Congress and five other states have also passed similar laws that aim to protect the personal information of public officials from disclosure. However, current state and federal legislation varies in scope and does not protect all public officials. For example, the federal-level Daniel Anderl Judicial Secrecy and Privacy Act only applies to current, senior, recalled, and retired Federal judges.[52] The CFPB's proposed rules would only permit covered data brokers to share information with third parties for permissible purposes. This limitation on disclosure would help to prevent personal information about public officials from being obtained by people who wish to harm public officials or their families.

---

[49] Alonzo Martinez, Protecting Public Officials: Impact of Judicial Privacy Laws on Background Checks, Forbes (May 31, 2024), https://www.forbes.com/sites/alonzomartinez/2024/05/31/protecting-public-officials-impact-of-judicial-privacy-laws-on-background-checks/.
[50] Justin Sherman, Data Brokers and Threats to Government Employees, Lawfare (Oct. 22, 2024), https://www.lawfaremedia.org/article/data-brokers-and-threats-to-government-employees.
[51] N.J. Stat. § 47:1B.
[52] 28 U.S.C. § 5933.

III. We support the CFPB's proposed rules.

We commend the Bureau for proposing rules which will establish many of the 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) de-identified data.

i. The CFPB is right to recognize that data brokers are covered by FCRA.

The CFPB is correct to recognize that many data brokers are consumer reporting agencies (CRAs) under the FCRA.[53] Because data brokers often engage in equivalent behaviors to CRAs or sell the same types of data as CRAs,[54] they must follow the same rules as CRAs. The CFPB's proposed rules would clarify FCRA coverage over data brokers by amending the definition of "consumer reports" and "consumer reporting agencies." These amendments would help to ensure that data brokers that sell certain categories of consumer data are correctly treated as CRAs and that data brokers that collect consumer information for permissible purposes under the FCRA may not sell the information for impermissible purposes.

Proposed Section 1022.4(c) expands on the phrase "is expected to be used," which is included in the definition of "consumer report." The Bureau proposes that information in a communication pertaining to a consumer's credit history, credit score, debt payments, or income or financial tier should always be expected to be used for a purpose included in Section 1022.4(a)(2), meaning that communication of this information by a CRA constitutes a consumer report. In addition to the categories of data listed in proposed Section 1022.4(c), EPIC encourages the Bureau to include the following additional categories of data in its final rules: employment history, court

[53] July Data Broker Comments at 51; October SBREFA Comments at 3.
[54] Protecting Americans from Harmful Data Broker Practices, Consumer Financial Protection Bureau, CFPB-2024-0044 (Dec. 3, 2024) [hereinafter Regulation V NPRM] at 11-12.

records, tenant history, and location data. Any communication by a CRA of these data categories should also be expected to be used for a permissible purpose authorized by FCRA, so these data categories should be specifically listed in Section 1022.4(c) along with credit history, credit score, debt payments, and income or financial tier.

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 specifically clarify that all data brokers are presumptively CRAs in the rule. The scope of FCRA is 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.[55] 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, 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.[56] 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

[55] *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).
[56] 15 U.S.C. § 1681a(d)(1).

constitute a consumer report if the record is used to make eligibility determinations.[57] 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.[58] Because data brokers are in the business of aggregating and selling consumer reports, they should presumptively be considered CRAs under the FCRA.

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 downstream consumer privacy, safety, and economic harms that the data broker industry causes, as explained in Section II of this comment. 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,[59] used to make inaccurate inferences about consumers,[60] and used to train and maintain harmful automated decision-making

[57] *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.").

[58] *See, e.g.*, *CLEAR Risk Inform*, Thomson Reuters, https://legal.thomsonreuters.com/en/products/clear-investigation-software/clear-risk-inform; *Credit Risk Assessment and Management*, LexisNexis Risk Solutions, 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).

[59] *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/.

[60] *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).

systems.[61] 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. The CFPB is right to recognize that credit header data is a consumer report.

EPIC and others have long urged the CFPB to promulgate rules that clarify that credit header data satisfies the definition of a consumer report when it is derived from data originating from a CRA and is data that is typically included in consumer reports issues by CRAs.[62] 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.[63] Credit header data is derived from CRA files and otherwise used in consumer reports, so it is a consumer report under the FCRA.[64]

We commend the Bureau for proposing rules to clarify that personally identifying data, often referred to as credit header data, constitutes a consumer report when the information was collected for the purpose of preparing consumer reports.[65] The rule should further clarify that consumer information from a CRA, regardless of content, is always a consumer report.[66]

We urge the Bureau to finalize rules that do not include any categorical exceptions for credit header information. Specifically, the NPRM invites input on including a law enforcement exemption to proposed § 1022.4(d). We urge the Bureau not to finalize rules with a law enforcement exemption to the credit header provisions because Section 608, Section 604(a), and Section 627 of the FCRA

---

[61] *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).
[62] Credit Header Letter; October SBREFA Comment at 6.
[63] 15 U.S.C. § 1681a(d)(1).
[64] Credit Header Letter.
[65] Regulation V NPRM at 16.
[66] *Id*.

already provide sufficient channels for law enforcement to access credit report data when necessary. If such an exemption must be included, we urge the Bureau to adopt a narrow provision, given that the FCRA already provides specific provisions related to law enforcement agencies' access to credit reporting information.

iii. The use of consumer reports for targeted marketing and advertising violates the FCRA.

As the NPRM 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.[67] As the NPRM also discusses, CRAs often work with third parties to combine consumer reports with third-party data and then deliver marketing and 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.[68] The CFPB should clarify in its final rules that such uses of consumer reports to deliver marketing materials on behalf of third parties is a violation of the FCRA.

iv. The CFPB should clarify the definition of de-identified data.

The NPRM also discusses how purportedly de-identified data can be aggregated with other data sets to reidentify individuals. The FCRA covers consumer data that can reasonably be linked to an individual, so when information is reasonably linkable to an individual, CRAs must be prohibited from disclosing data without a permissible purpose. We commend the Bureau for carefully considering three proposals to ensure that the FCRA correctly defines de-identified data. We recommend that the Bureau adopt Proposed Alternative One[69] in the final rule because this proposal

[67] Regulation V NPRM at 94, 109-112.
[68] July Data Broker Comments at 68-71.
[69] Regulation V NPRM at 70.

best protects consumer privacy. Proposal One eliminates the risk of de-identified data being used improperly by making no distinction between de-identified and identifiable data when the information being communicated by a CRA would constitute a consumer report if the information were not de-identified.[70] Aggregated or nominally "anonymized" data can often be linked to an individual when it is combined with other data and used to reidentify an individual. Given the difficulty of determining whether de-identified information could be re-identified, the Bureau should finalize rules that make no distinction between de-identified and identifiable information.

IV. Recommended additions

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

Though the Bureau considered including specific data security protections in its September Outline of Proposals and Alternatives Under Consideration, the NPRM does not include these. We encourage the Bureau to include explicit data security protections in the final rules because the FCRA must meet modern data security challenges, especially given the massive risk of harm to

[70] Regulation V NPRM at 69.

consumers posed by breaches of personal information. We recommend that the Bureau adopt the following non-exhaustive list of provisions in the final rules.

First, we urge the Bureau to require that CRAs 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.[71]

Second, the rule should further incorporate principles of data minimization.[72] For example, 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 also 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.[73]

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.[74]

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,"[75] 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.[76] When data that is covered by the FCRA is combined with non-covered data, the combined

[71] July Data Broker Comments at 61-63.
[72] 16 C.F.R. § 682.1(c)(1).
[73] January Financial Data Rights Comments at 6.
[74] July Data Broker Comments at 58.
[75] 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.
[76] *Id*. at 54–55.

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 privacy tools.[77] 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 recently updated Safeguards Rule. Those standards include access controls, secure password practices, user authentication, system segmentation, traffic monitoring, staying current on known vulnerabilities, security reviews, and employee training.[78] 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.[79] We recommend that the CFPB incorporate similar data breach notification requirements into the rule.

ii. Know-your-customer protocols

As the Bureau notes in its NPRM,[80] 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, the risk of data breach, and the risk that data will be used to train and

[77] *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/.
[78] 16 C.F.R. 314.4; January Financial Data Rights Comments at 17–18.
[79] *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/.
[80] Regulation V NPRM.

deploy harmful algorithmic decision-making tools. We recommend that the final rule require data brokers to use know-your-customer (KYC) protocols to mitigate downstream misuse of data.[81] This would require CRAs to undertake ongoing monitoring of users of consumer reports, which builds on existing FCRA due diligence requirements.[82]

iii. Protections against the use of alternative data in credit scoring models

When finalizing rules 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,[83] and the Commission has noted that data not traditionally associated with creditworthiness (e.g., ZIP code, social media usage, shopping history, and 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.[84]

In the NPRM, the Bureau states that data types not listed in proposed § 1022.4(c)(2), including alternative data, could still be a consumer report if the entity communicating the information expects or should expect that the recipient will use the information for an FCRA purpose.[85] We recommend the Bureau to include specific language in the final rule clarifying 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.[86]

---

[81] July Data Broker Comments at 59; October SBREFA Comments at 3-5, 10.
[82] *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.
[83] *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.
[84] *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.
[85] Regulation V NPRM at 46.
[86] July Data Broker Comments at 66; October SBREFA Comments at 10.

iv. 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 final rule.[87] Credit reports often contain errors, are not up to date, and do not reflect a consumer's current ability to pay.[88] 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, *2024 Consumer Reform Priorities to Protect Tenants*.[89]

v. Ban the use of pre-conviction criminal proceeding information in credit reports.

Similar to using credit reports in tenant screening, using pre-conviction criminal proceeding information such as arrest records in credit reporting also introduces inaccuracy and perpetuates inequality.[90] 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 their creditworthiness or eligibility for other benefits.[91] Evidence shows that arrest statistics are influenced

[87] *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/.

[88] *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 Feb. 11, 2025); 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.

[89] 2024 Consumer Reform Priorities to Protect Tenants, National Consumer Law Center (Mar. 2024), https://www.nclc.org/wp-content/uploads/2023/02/202403_Issue-Brief_2024-Consumer-Reform-Priorities-to-Protect-Tenants.pdf.

[90] July Data Broker Comments at 67.

[91] *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).

by racial bias, and using pre-conviction criminal proceeding data perpetuates that bias and introduces inaccuracy into credit reporting.[92] We urge the CFPB to prohibit the use of pre-conviction data in credit reports to better protect consumers.

V. Conclusion

We commend the CFPB's work to strengthen protections for consumers in data broker and consumer reporting industries. As this comment details, consumers experience significant harm from exploitative data collection, sharing, and use practices; improper data security protections, discriminatory uses of credit reporting data; and downstream misuse of consumer data. The Bureau's proposed rules present an opportunity to update FCRA regulations to better protect consumers in the modern credit reporting ecosystem. We appreciate this opportunity to comment. If you have any questions, please contact EPIC Law Fellow Caroline Kraczon (kraczon@epic.org).

Respectfully Submitted,

Electronic Privacy Information Center

National Consumers League

Consumer Federation of America

Joined by:

Brennan Center for Justice

Center on Race and Digital Justice

[92] *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.

Check My Ads Institute

Fight for the Future

Just Futures Law

Mijente

National Consumer Law Center (on behalf of its low-income clients)

UltraViolet Action