April 10, 2025

Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552
Via www.regulations.gov

Re: Docket Number CFPB-2025-0005, Request for Information Regarding the Collection, Use, and Monetization of Consumer Payment and Other Personal Financial Data

The National Consumer Law Center ("NCLC"), on behalf of its low-income clients, and the Electronic Privacy Information Center (EPIC) are pleased to respond to the Consumer Financial Protection Bureau's (CFPB) Request for Information Regarding the Collection, Use, and Monetization of Consumer Payment and Other Personal Financial Data.[1]

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has worked for consumer justice and economic security for low-income and other disadvantaged people in the United States through its expertise in policy analysis and advocacy, publications, litigation, expert witness services, and training. The Electronic Privacy Information Center (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. Without clear, strong consumer protections, consumers are harmed by the collection, use, and monetization of consumer payment and other personal financial data.

It is undeniable that in the past decade, the United States has seen a wide variety of new types of payment mechanisms offered by non-traditional banking and payment companies. The lack of clarity of consumer financial protection laws that apply to these emerging payment mechanisms

[1] *See* CFPB, Request for Information Regarding the Collection, Use, and Monetization of Consumer Payment and Other Personal Financial Data, 90 Fed Reg. 3804 (Jan. 15, 2025). These comments were written by NCLC Senior Attorney Carla Sanchez-Adams, with assistance from Chi Chi Wu, NCLC Senior Attorney.

subject consumers to more risk and, therefore, potentially greater harm.[2]

Simultaneously, the market for the sale of consumer data has exploded in the past few decades. Companies collect and sell information harvested from payment transactions including consumers' locations and buying habits. Data gets sold and resold without any meaningful consent from the consumer.

The data industry has existed for decades, if not centuries, but current technology allows companies to collect, store, and interconnect data in ways that were not possible before. Today, the "dossier" industry is bigger than ever. In 2021, the market for "data brokers" was valued at $240.3 billion. [3] It is expected to reach $462.4 billion by the end of 2031.[4]

Data brokers sell all manner of information about individuals, going far beyond the actual or "raw" data (e.g., an individual's name, address, age, ethnicity, occupation, and income).[5] Data brokers combine scores of datasets to create a "mosaic" of "where we go, who we know, and what we do each day."[6] Data brokers offer potential buyers pre-packaged databases of information organized around certain consumer preferences or predictive behaviors.[7] "By tailoring their services for different purposes, data brokers sell products to various types of customers," such as advertising and marketing, credit and insurance, identity verification and fraud detection, health care, education, government agencies, law enforcement, and customer services.[8]

Yet the way these companies operate is intentionally opaque.[9] Some companies obtain non-public consumer information provided by consumers to the companies from which they obtain

---

[2] *See* NCLC, et.al. Comments to the CFPB's Proposed Rule Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, Docket No. CFPB-2023-0053 (Jan. 8, 2024), available at https://www.nclc.org/wp-content/uploads/2024/01/240108-CFPB-Payments-App-Comment-Final.pdf.

[3] Data brokerage is generally defined as, "the practice of buying, aggregating, selling, licensing, and otherwise sharing individuals' data." *See* Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, Duke Sanford Cyber Policy Program (Aug. 2021) (hereinafter "*Sherman, Data Brokers and Sensitive Data*").

[4] Press Release, *Data Brokers Market Estimated to Reach US$ 462.4 billion by 2031, TMR Report*, GlobeNewswire (Aug. 1, 2022), available at https://www.globenewswire.com/news-release/2022/08/01/2489563/0/en/Data-Brokers-Market-Estimated-to-Reach-US-462-4-billion-by-2031-TMR-Report.html.

[5] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (2014), at 19, available at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf ("For example, a data broker might infer that an individual with a boating license has an interest in boating, that a consumer has a technology interest based on the purchase of a Wired magazine subscription, that a consumer has an interest in shoes because she visited Zappos.com, or that a consumer who has bought two Ford cars has loyalty to that brand.").

[6] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, Yale Law Journal 115, no. 3 (Dec. 2005), 628-79.

[7] Sherman, *Data Brokers and Sensitive Data*, at 2; FTC, *Data Brokers*, at 19.

[8] Chih-Liang Yeh, *Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers*, Telecommunications Policy 42, no. 4 (Dec. 2017), at 285 (hereinafter "Yeh, *Pursuing consumer empowerment*").

[9] "Many data brokers admit that their work is a black box because of the 'veil of secrecy surrounding the origins of the information, how it is analyzed, and who buys it.'" *See* Yeh, *Pursuing consumer empowerment*, at 288. (quoting Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money And Information* (2015), MA: Harvard Univ. Press, at 33).

products or services, (including data harvested from payment transactions and a consumer's purchase history). These companies may gather this data directly from firms they own,[10] or "purchase, license, or otherwise acquire data second-hand from companies that directly collect this information from their users."[11]

Furthermore, the CFPB observed that:

- actual business practices show significant deviation from longstanding consumer expectations when it comes to the collection, use, and monetization of data harvested from payment transactions;
- companies operating payment systems and apps are able to connect payments data with a broad range of other data;
- there have been significant advances in the capabilities of physical devices and hardware, giving these companies the technical capability to collect biometric information (including certain vital signs and the voices of individuals proximate to the primary user), geographic location, social networking habits, and more; and
- the commingling of this data with personal financial data could lead to such information being used to develop dynamic pricing algorithms that tailor prices to a particular individual, where the seller is aided by knowledge about the consumer's purchase history.[12]

This collection, use, and monetization of consumer payment and other personal financial data without clear consumer protection leads to consumer harm. Consumers are besieged with unwanted written solicitations and phone calls; this harassing behavior is not only annoying but also interferes with consumers' ability to be reached by contacts they do want to hear from. Additionally, the data that is sold or shared with other companies provides the fuel for targeted marketing and direct solicitations that can lead to consumers falling victim to scams. Data collected by companies may also lead to privacy breaches and identity theft. Data collected by companies may be inaccurate, leading to adverse actions like account closures, denials of demand deposit accounts, higher costs of products or services, or reputational injury.

Additionally, the lack of transparency about the collection, use, and monetization of consumer payment and other personal financial data is its own form of harm. Companies collect and sell consumer data without the consumer's consent, so that "most people are unaware of [data brokers'] existence and their substantial impact on daily transactions."[13] This opaqueness not only compounds the above-referenced problems but also prevents a consumer from correcting any errors in information shared about them, especially when the consumer is not even aware of the existence of the data collected, the way it is shared, or to whom it is shared.

---

[10] Sarah Lamdan, *Data Cartels: The Companies That Control and Monopolize Our Information* (2003), Stanford University Press, at 3, 7 (describing Thomson Reuters and Reed Elsevier LexisNexis (RELX) as "conglomerates, multi-industry behemoths that control swaths of resources" and "capitalize on the troves of materials that they get through taking over competitors").

[11] Sherman, *Data Brokers and Sensitive Data*, at 2.

[12] 90 Fed Reg. 3804, 3804 (Jan. 15, 2025).

[13] Yeh, *Pursuing consumer empowerment*, at 283.

2. The Fair Credit Reporting Act best addresses consumer harm from the collection, use, and monetization of consumer payment and other personal financial data.

Given the sensitive information collected, used, and monetized by companies as described above and the risks of harm to consumers from the improper disclosure of accurate information as well as the propagation of inaccurate information, appropriate regulation is extremely important. No one law governs all the various uses of the information collected by these companies, but any proposed changes to Regulation P, which implements the Gramm Leach Bliley Act (GLBA), would be insufficient to protect consumers from these harms. The Fair Credit Reporting Act (FCRA) has the most robust protections for consumers.

Among other things, the FCRA:

- *Provides consumers the right to access information collected and shared about them by a consumer reporting agency*. 15 U.S.C. § 1681g
- *Requires that information shared about consumers be accurate:* the FCRA requires "reasonable procedures for maximum possible accuracy" from entities preparing and sharing consumer reports. 15 U.S.C. § 1681e(b)
- *Provides privacy protections to prevent inappropriate dissemination and use of consumer information:* only users with a "permissible purpose" can access consumer reports. 15 U.S.C. § 1681b
- *Provides consumers the right to know when information is used against them:* consumers receive an "adverse action" notice when information in the form of a consumer report is used to deny them credit, employment, insurance, rental housing, or many other financial essentials. 15 U.S.C. § 1681m.
- *Provides consumers the right to correct errors:* consumers have the right to dispute inaccurate information and get it corrected. 15 U.S.C. §§ 1681i(a), 1681s-2(a)(8), 1681s-2(b)
- *Provides protection to victims of identity theft.* 15 U.S.C. §§ 1681c-1, 1681c-2

These protections are critical to prevent privacy and inaccuracy violations that significantly harm consumers. Thus, as discussed below, we urge the CFPB to finalize its proposed rule to regulate many data brokers under the FCRA.

3. The CFPB should finalize its Proposed Rule Regarding Protecting Americans from Harmful Data Broker Practices issued December 13, 2024.

Because the FCRA has the most robust protections for consumers when their payment and other personal financial data is collected, used, and monetized, the CFPB should clarify that the companies that collect and sell this information are consumer reporting agencies and that the information they collect and sell to others is a consumer report.

As discussed in more detail in other NCLC comments,[14] the FCRA contains a very broad definition of a "consumer report" and "consumer reporting agency". These broad definitions

[14] *See* NCLC Comments to the CFPB's Proposed Rule Regarding Protecting Americans From Harmful Data Broker Practices (Regulation V), Docket No. CFPB–2024–0044 (Mar. 28, 2025) available at https://www.nclc.org/wp-

reflect the enacting Congress's concern about the ever-expanding "information network" and unchecked "dossier industry,"[15] which was disseminating information about individuals' financial status, criminal history, and general reputation without "public regulation or supervision."[16] With these concerns in mind, Congress passed the FCRA in order "to enable consumers to protect themselves against [such] arbitrary, erroneous, and malicious" information.[17]

Privacy and confidentiality issues were among the chief concerns that led Senator William Proxmire, considered the father of the FCRA, to introduce the first version of the Act. At the time, some consumer reporting agencies would sell information to virtually anyone,[18] and the information they obtained was used in ways inconsistent with the purpose for which it was collected. The need for FCRA coverage of data brokers is even more urgent today. The data industry, already well developed when the FCRA became law in 1970, has exploded in the decades since. The technology available now allows companies to collect, store, and interconnect data in ways that were not possible before.

The FCRA covers companies collecting, using, and monetizing consumer payment and other personal financial data when they meet the definition of a consumer reporting agency and the product they are selling meets the statutory definition of a consumer report. A consumer reporting agency (CRA) is defined by the Act as:

> [A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. 15 U.S.C. § 1681a(f)

Thus, a company is a CRA covered by the statute if it engages in the practice of assembling or evaluating one of the seven categories of information for the purpose of furnishing consumer reports. A consumer report, in turn, is defined as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or

---

content/uploads/2025/04/2025.03.28_Comments_NCLC-Comments-to-the-CFPB-NPRM-on-data-brokers.pdf; NCLC Response to the CFPB's Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, Docket No. CFPB–2023- 0020 (Jul. 14, 2023), available at https://www.nclc.org/wp-content/uploads/2023/07/NCLC-Comments-to-CFPB-RFI-on-Data-Brokers-Chi-Chi-Wu.pdf; and NCLC Comments to the CFPB's Outline of Proposals for Consumer Reporting Rulemaking, Small Business Regulatory Enforcement Fairness Act Review (Nov. 9, 2023), available at https://www.nclc.org/wp-content/uploads/2023/11/NCLC-Comments-to-SBREFA-Outline-of-Proposals-for-the-FCRA-Rulemaking.pdf.

[15] Robert M. McNamara Jr., The Fair Credit Reporting Act: A Legislative Overview, 22 J. Pub. L. 78, 80 (1973) (quoting Nader, *The Dossier Invades the Home*, Saturday Rev., Apr. 17, 1971, at 18–21).

[16] 115 Cong. Rec. 2410 (1969).

[17] *Id*.

[18] National Consumer Law Center, *Fair Credit Reporting* § 1.4 (10th ed. 2022), updated at www.nclc.org/library.

expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for--
(A) credit or insurance to be used primarily for personal, family, or household purposes;
(B) employment purposes; or
(C) any other purpose authorized under section 1681b of this title.
15 U.S.C. § 1681a(d)(1).

The first part of the definition of consumer report, whether the information in question bears on one of the seven factors, is usually not in question, and definitely would not be in the case of consumer payment and other personal financial data collected by payment apps.

The second part of the definition of consumer report, how the data is "used or expected to be used or collected," is where there has been much debate and litigation, and which creates the need for CFPB to issue firm rules. A data product is a consumer report, and the provider will be a CRA, if the data is either (1) used, (2) expected to be used, or (3) collected "in whole or in part" for the purpose of serving as a factor in establishing the consumer's eligibility for credit, insurance, employment, or some other permissible purpose listed in Section 1681b. Those other permissible purposes include sale:

(3) To a person which it [the CRA] has reason to believe–

(A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or
(B) intends to use the information for employment purposes; or
(C) intends to use the information in connection with the underwriting of insurance involving the consumer; or
(D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or
(E) intends to use the information, as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; or
(F) otherwise has a legitimate business need for the information--
(i) in connection with a business transaction that is initiated by the consumer; or
(ii) to review an account to determine whether the consumer continues to meet the terms of the account.
(G) executive departments and agencies in connection with the issuance of government-sponsored individually-billed travel charge cards.
15 U.S.C. § 1681b(a).

These permissible purposes are quite broad, and in turn, the definition of a consumer report should be equally broad. If information is either used or expected to be used or collected for one of the covered purposes listed in § 1681b(a), then the FCRA should apply and the CRA may *only* sell the information for a permissible purpose.

As a result, the CFPB should finalize its Proposed Rule Regarding Protecting Americans from Harmful Data Broker Practices. The rule will provide much-needed protection to address the harms and problems associated with the collection, use, and monetization of consumer payment and other personal financial data. It will prevent evasion by data brokers who claim they are merely "conduits" of information. The rule will also provide strong guardrails for the sharing of consumer data; when businesses obtain a consumer's written authorization to obtain a credit or other consumer report, they will need to ensure the consent is active, knowing, and subject to strong protections.

4. The CFPB should collect data and publish reports about the collection, use, and monetization of consumer payment and other personal financial data.

As previously mentioned, there is limited information about how companies collect, use, and monetize consumer payment and other financial data. As a result, the CFPB should collect the following information: [19]

- What consumer payment and other financial data is collected by these companies;
- How the collected information is processed and analyzed;
- Whether the information collected is aggregated or anonymized;
- What types of entities the companies collecting consumer payment and other financial data sell the information to, including the names of the purchasing entities where possible;
- How much revenue the companies selling consumer payment and other financial data generate from the sale of this information; and
- What safeguards or requirements the companies selling consumer payment and other financial data impose on buyers in terms of security, resale, and usage, especially for FCRA covered purposes.

The CFPB should also collect the contracts between the companies that sell consumer payment and other financial data and the buyers.

After collecting this information, the CFPB should then publish general reports about how companies that collect, use, and monetize consumer payment and other financial data treat the data harvested from consumer payment transactions.

5. Conclusion

Consumers need clarity about their rights when companies collect, use, and monetize their payment and personal financial data. Without strong consumer protections, consumers will be harmed when that information is shared and used to make decisions about the consumer-particularly when that information may be incorrect. Consumers need to be able to correct any errors in information shared about them, especially when the consumer is not even aware of the existence of the data collected, the way it is shared, or to whom it is shared.

[19] This is responsive to Question 12 of the RFI. *See* 90 Fed Reg. 3804, 3808 (Jan. 15, 2025).

The Fair Credit Reporting Act best addresses these challenges. The CFPB's Proposed Rule Regarding Proposed Rule Regarding Protecting Americans From Harmful Data Broker Practices issued December 13, 2024, would clarify that consumers have the protections of the FCRA when companies such as data brokers collect, use, and monetize their payment and personal financial data. As such, the CFPB should finalize the proposed rule.

Additionally, more transparency in how consumer payment and other personal financial data is collected, sold, and monetized is needed. The CFPB needs to collect and publish more information about the companies that collect, use, and monetize consumer payment and other personal financial data and how that data is collected and used.

We welcome questions on this matter, directed to Carla Sanchez-Adams at csanchezadams@nclc.org or Chi Chi Wu at cwu@nclc.org. Thank you for your consideration.

Sincerely,

National Consumer Law Center, on behalf of its low-income clients
Electronic Privacy Information Center