Specifically, the proposed rule would lower the immunity provision for late fees to $8 for a missed payment and end the automatic annual inflation adjustment. The proposed rule would also ban late fee amounts above 25% of the consumer's required payment.

3.1.2 CFPB Issued Circular on Unanticipated Overdraft Fee Assessment Practices

On October 26, 2022, the CFPB issued guidance indicating that overdraft fees may constitute an unfair act or practice under the CFPA, even if the entity complies with the Truth in Lending Act (TILA) and Regulation Z, and the Electronic Fund Transfer Act (EFTA) and Regulation E.[22] As detailed in the circular, when financial institutions charge surprise overdraft fees, sometimes as much as $36, they may be breaking the law. The circular provides some examples of potentially unlawful surprise overdraft fees, including charging fees on purchases made with a positive balance. These overdraft fees occur when a bank displays that a customer has sufficient available funds to complete a debit card purchase at the time of the transaction, but the consumer is later charged an overdraft fee. Often, the financial institution relies on complex back-office practices to justify charging the fee. For instance, after the bank allows one debit card transaction when there is sufficient money in the account, it nonetheless charges a fee on that transaction later because of intervening transactions.

3.1.3 CFPB Issued Bulletin on Unfair Returned Deposited Item Fee Assessment Practices

On October 26, 2022, the CFPB issued a bulletin [23] stating that blanket policies of charging returned deposited item fees to consumers for all returned transactions irrespective of the circumstances or patterns of behavior on the account are likely unfair under the CFPA.

3.1.4 CFPB Issued Advisory Opinion on Debt Collectors' Collection of Pay-to-Pay Fees

On June 29, 2022, the CFPB issued an advisory opinion [24] affirming that Federal law often prohibits debt collectors from charging ''pay-to-pay'' fees. These charges, commonly described by debt collectors as ''convenience fees,'' are imposed on consumers who want to make a payment in a particular way, such as online or by phone.

4. Remedial Actions

4.1 Public Enforcement Actions

The Bureau's supervisory activities resulted in and supported the following enforcement action.

4.1.1 Wells Fargo

On December 20, 2022, the CFPB and Wells Fargo entered into a consent order in which Wells Fargo will pay more than $2 billion in redress to consumers and a $1.7 billion civil penalty for legal violations across several of its largest product lines.[25] The bank's illegal conduct led to billions of dollars in financial harm to its customers and, for thousands of customers, the loss of their vehicles and homes. Consumers were illegally assessed fees and interest charges on auto and mortgage loans, had their cars wrongly repossessed, and had payments to auto and mortgage loans misapplied by the bank. Wells Fargo also improperly froze or closed customer deposit accounts, charged consumers unlawful surprise overdraft fees, and did not always waive monthly account service fees consistent with its disclosures. Under the terms of the order, Wells Fargo will pay redress to the over 16 million affected consumer accounts, and pay a $1.7 billion fine, which will go to the CFPB's Civil Penalty Fund, where it will be used to provide relief to victims of consumer financial law violations.

4.1.2 Regions Bank

On September 28, 2022, the CFPB ordered Regions Bank to pay $50 million into the CFPB's victims relief fund and to refund at least $141 million to customers harmed by its illegal surprise overdraft fees.[26] Until July 2021, Regions charged customers surprise overdraft fees on certain ATM withdrawals and debit card purchases. The bank charged overdraft fees even after telling consumers they had sufficient funds at the time of the transactions. The CFPB also found that Regions Bank leadership knew about and could have discontinued its surprise overdraft fee practices years earlier, but they chose to wait while Regions pursued changes that would generate new fee revenue to make up for ending the illegal fees.

This is not the first time Regions Bank has been caught engaging in illegal overdraft abuses. In 2015, the CFPB found that Regions had charged $49 million in unlawful overdraft fees and ordered Regions to make sure that the fees had been fully refunded and pay a $7.5 million penalty for charging overdraft fees to consumers who had not opted into overdraft protection and to consumers who had been told they would not be charged overdraft fees.[27]

Rohit Chopra,

Director, Consumer Financial Protection Bureau.

[FR Doc. 2023–05667 Filed 3–20–23; 8:45 am]

BILLING CODE 4810–AM–P

[22] Consumer Financial Protection Circular 2022–06, Unanticipated Overdraft Fee Assessment Practices (Oct. 26, 2022), available at: *https://files.consumerfinance.gov/f/documents/cfpb_unanticipated-overdraft-fee-assessment-practices_circular_2022-10.pdf.*

[23] Bulletin 2022–06: Unfair Returned Deposited Item Fee Assessment Practices, available at: *https://files.consumerfinance.gov/f/documents/cfpb_returned-deposited-item-fee-assessment-practice_compliance-bulletin_2022-10.pdf.*

[24] Advisory Opinion on Debt Collectors' Collection of Pay-to-Pay Fees, available at: *https://files.consumerfinance.gov/f/documents/cfpb_convenience-fees_advisory-opinion_2022-06.pdf.*

[25] CFPB Consent Order 2022–CFPB–0011, In the Matter of Wells Fargo Bank (Dec. 20, 2022), available at: *https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.*

[26] CFPB Consent Order 2022–CFPB–0008, In the Matter of Regions Bank (Sept. 28, 2022), available at: *https://files.consumerfinance.gov/f/documents/cfpb_Regions_Bank-_Consent-Order_2022-09.pdf.*

[27] CFPB Consent Order 2015–CFPB–0009, In the Matter of Regions Bank (Apr. 28, 2015), available at: *https://files.consumerfinance.gov/f/201504_cfpb_consent-order_regions-bank.pdf.*

BUREAU OF CONSUMER FINANCIAL PROTECTION

[Docket No. CFPB–2023–0020]

Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information

AGENCY: Bureau of Consumer Financial Protection.

ACTION: Request for public comment.

SUMMARY: The Consumer Financial Protection Bureau (CFPB) is seeking comments from the public related to data brokers. The submissions in response to this request for information will serve to assist the CFPB and policymakers in understanding the current state of business practices in exercising enforcement, supervision, regulatory, and other authorities.

DATES: Comments must be received on or before June 13, 2023.

ADDRESSES: You may submit comments, identified by Docket No. CFPB–2023–0020, by any of the following methods:

- *Federal eRulemaking Portal: https://www.regulations.gov.* Follow the instructions for submitting comments.
- *Email: DataBrokersRFI_2023@cfpb.gov.* Include the document title and Docket No. CFPB–2023–0020 in the subject line of the message.
- *Mail/Hand Delivery/Courier:* Comment Intake, Request for Information Regarding Data Brokers, Consumer Financial Protection Bureau, c/o Legal Division Docket Manager, 1700 G Street NW, Washington, DC 20552. Because paper mail in the Washington, DC area and at the CFPB is subject to delay, commenters are encouraged to submit comments electronically.

Instructions: The CFPB encourages the early submission of comments. All submissions should include the agency name and docket number for this request for information. Please note the number of the topic on which you are commenting at the top of each response (you do not need to address all topics.) In general, all comments received will be posted without change to *https://www.regulations.gov.* All comments, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, should not be included. Comments generally will not be edited to remove any identifying or contact information.

FOR FURTHER INFORMATION CONTACT: Erie Meyer, Chief Technologist and Senior Advisor, Office of the Director; Davida Farrar, Counsel, Office of Consumer Populations at 202–435–7700. If you require this document in an alternative electronic format, please contact *CFPB_Accessibility@cfpb.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

In 1970, Congress enacted the Fair Credit Reporting Act (FCRA),[1] one of the first data privacy laws in the world. The primary sponsor of the legislation, Senator William Proxmire, at the time publicly described an emerging consumer reporting market involving the dissemination of a wide range of information about Americans, including financial status, bill paying records, public records including arrests, suits, and judgments, dossiers, information on drinking, marital discords, adulterous behavior, general reputation, habits, and morals. The Senator stressed that ''while the growth of this information network is somewhat alarming, what is even more alarming is the fact that the system has been built with virtually no public regulation or supervision.'' [2]

Before voting on the FCRA, Congress held a series of investigative hearings and uncovered a wide variety of abuses in the industry. For example, Congress found that many consumers were unaware of the existence of the industry because non-disclosure agreements between consumer reporting agencies and users hid the arrangement behind a shroud of secrecy.[3] In addition, the hearings revealed the practice of including disclaimers of accuracy in agreements between consumer reporting agencies and creditors; before the FCRA, consumer reporting agencies purported to be mere transmitters of information who were not responsible for accuracy.[4] Congress also criticized the fact that consumers were not given access to their credit reports,[5] and that credit reports often included obsolete or irrelevant information.[6]

Ultimately, Congress found that consumer reporting agencies assumed a vital role in assembling and evaluating consumer credit and other information on consumers to meet the needs of commerce, but that rules were necessary to ensure they handed information fairly and equitably with regard to confidentiality, accuracy, relevancy, and proper use.[7] The FCRA established comprehensive rules to govern the practices of consumer reporting agencies, including four key features: (1) a prohibition on using or disseminating certain personal data outside prescribed permissible purposes selected by Congress,[8] (2) a requirement that consumer reporting agencies ''follow reasonable procedures to assure maximum possible accuracy'' of consumer reports,[9] (3) a right of consumers to inspect data about themselves,[10] and (4) due process to challenge false data.[11]

The FCRA still remains on the books and has been amended from time to time.[12] But since the enactment of the FCRA, companies using business models that sell consumer data have emerged and evolved with the growth of the internet and advanced technology. Many companies whose business models rely on newer technologies and novel methods purport not to be covered by the FCRA. These companies are sometimes labeled ''data brokers,'' ''data aggregators,'' or ''platforms,'' but they all share a fundamental characteristic with consumer reporting agencies—they collect and sell personal data.

With the passage of the Consumer Financial Protection Act (CFPA), Congress transferred rulemaking authority for most provisions of the FCRA from the Federal Trade Commission to the CFPB. The CFPA granted the CFPB the authority to enforce the FCRA along with other Federal regulators.[13] The CFPA also granted the CFPB various additional authorities that may be applicable to companies that collect and sell personal data, including, for example, authorities pursuant to the Gramm-Leach Bliley Act's privacy provisions.[14] The CFPB has used its authority to address unfair or deceptive acts or practices related to the handling of consumer data.[15]

This request for information is seeking information to (1) help inform the CFPB about new business models that sell consumer data, including information relevant to assessments of whether companies using these new business models are covered by the FCRA, given the FCRA's broad definitions of ''consumer report'' and ''consumer reporting agency,'' [16] or other statutory authorities, and (2) collect information on consumer harm and any market abuses, including those that resemble harms Congress originally identified in 1970 in passing the FCRA.

II. Overview

Data brokers is an umbrella term to describe firms that collect, aggregate, sell, resell, license, or otherwise share consumers' personal information with other parties. Data brokers encompass actors such as first-party data brokers

[1] 15 U.S.C. 1681 *et seq.*

[2] 115 Cong. Rec. 2410 (1969).

[3] Robert M. McNamara Jr., *The Fair Credit Reporting Act: A Legislative Overview,* 22 J. Pub. L. 67, 80 (1973).

[4] Hearing on Retail Credit Co. of Atlanta, Ga., Before a Subcomm. on Invasion of Privacy of the House Comm. on Government Operations, 90th Cong., 2d Sess. 47 (1968).

[5] Hearings on Commercial Credit Bureaus Before a Subcomm. on Invasion of Privacy of the House Comm. on Government Operations, 90th Cong., 2d Sess. 10 (1968).

[6] *See* S. Rep. No. 517, 91st Cong., 1st Sess. 4 (1969).

[7] 15 U.S.C. 1681 (Congressional findings and statement of purpose for FCRA).

[8] 15 U.S.C. 1681b.

[9] 15 U.S.C. 1681e(b).

[10] 15 U.S.C. 1681g.

[11] 15 U.S.C. 1681i, 1681s–2.

[12] Consumer Credit Reporting Reform Act of 1996, Pub. L. 104–208 (1996).

[13] *See* 15 U.S.C. 1681s.

[14] *See, e.g.,* 12 U.S.C. 5481(12)(J) (specifying provisions of the Gramm-Leach-Bliley Act that qualify as ''enumerated consumer laws'' over which the Bureau has jurisdiction).

[15] *See, e.g.,* Consumer Financial Protection Circular 2022–04, *Insufficient data protection or security for sensitive consumer information, https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.*

[16] *See* 15 U.S.C. 1681a(d), (f).

that interact with consumers directly, as well as third-party data brokers with whom the consumer does not have a direct relationship. Data brokers include firms that specialize in preparing employment background screening reports and credit reports. Data brokers collect information from public and private sources for purposes including marketing and advertising, building and refining proprietary algorithms, credit and insurance underwriting, consumer-authorized data porting, fraud detection, criminal background checks, identity verification, and people search databases.[17]

As part of the CFPB's statutory mandate to promote fair, transparent, and competitive markets for consumer financial products and services, this request for information is part of a series of efforts to examine data collection and use. In addition to supervision of consumer reporting agencies, including the three largest nationwide consumer reporting agencies, the CFPB endeavors to gain insight into the full scope of the data broker industry. The data broker industry is growing and expanding its reach into new spheres of consumers' personal lives, as more sophisticated computerization has increased the power of these companies to track and predict consumer behavior. Yet, many people lack an understanding of the scope and breadth of data brokers' business practices and the impact of those practices on the marketplace and peoples' daily lives.

The CFPB seeks to better understand the heterogeneity of these firms and to assist firms in understanding any compliance obligations under the FCRA and other laws as appropriate.

Data brokers collect or share a vast range of information, often building profiles of individuals by delving into the details of consumers' everyday interactions, including credit card purchases and web browsing activity. Data brokers also collect other types of sensitive and intimate personal information such as genetic and health information, religious affiliation, financial records, and geolocation data.[18]

Government agencies, technology and privacy experts, financial institutions, consumer advocates, and others have identified numerous consumer harms and abuses related to the operation of data brokers, including significant privacy and security risks, the facilitation of harassment and fraud, the lack of consumer knowledge and consent, and the spread of inaccurate information.[19]

People should be able to expect companies to safeguard their most personal and intimate information, and should be able to have knowledge and control over how companies obtain and use their data. Surveys have found that people are concerned about being tracked and surveilled by companies, and express concern about the lack of control over how data collected about them is used.[20]

While observers have documented the increasing role of data brokers in the economy, there is still relatively limited public understanding of their operations and other impacts.

III. Request for Information

This request for information seeks comments from the public on data brokers. The CFPB welcomes stakeholders to submit data, analysis, research, and other information about data brokers. The CFPB also requests input from individuals who have interacted with or have been affected by data broker business practices. To assist commenters in developing responses, the CFPB has crafted the below questions that commenters may answer. However, the CFPB is interested in receiving any comments relating to data brokers.

Market-Level Inquiries

1. What types of data do data brokers collect, aggregate, sell, resell, license, derive marketable insights from, or otherwise share?

a. What do data brokers do with the data they collect other than the aggregation, selling, reselling, or licensing of data?

b. Please provide information about specific types of data that are financial in nature, such as information about salary, income sources, spending, investments, assets, use of financial products or services, investments, signals of financial distress, etc.

2. What sources do data brokers rely on to collect information? What collection methods do data brokers use to source information?

a. What specific types of information do data brokers obtain from public records databases? Which public records sources do data brokers use?

b. Are people unknowingly deceived or manipulated into supplying data to data brokers? Describe the nature of such deception or manipulation.

c. What technological components facilitate brokers' collection of data, including but not limited to: tracking scripts, web-based plug-ins, pixels, or software development kits (SDKs) in Apps?

3. What specific types of information do data brokers receive from financial institutions? Do financial institutions place any restrictions on the use of this data? Under what circumstances do consumers consent to this data sharing or receive an opportunity to opt-out of this sharing?

4. What specific entities and types of entities have relationships (*e.g.,* partnerships, vendor relationships, investor relationships, joint ventures, retail arrangements, data share agreements, third-party pixel usage) with data brokers? Describe the nature of those relationships and any relevant financial arrangements pursuant to such relationships.

5. Which specific entities and types of entities collect, aggregate, sell, resell, license, or otherwise share consumers' personal information with other parties?

6. Does the granular nature of data brokers' collection of information related to consumer preferences and behaviors influence consumer purchasing patterns or levels of indebtedness? Describe the nature of such collection and how it may influence purchasing patterns.

7. How do companies collect consumer data to create, build, or refine proprietary algorithms?

8. Does consumer data collected by data brokers facilitate a less competitive marketplace or more expensive financial products for consumers, and if so, how?

9. Can people avoid having their data collected?

a. Are there certain special populations that are less likely to be able to exercise control over the collection, aggregation, sale, resale, licensing, or other sharing of their data?

b. If so, which special populations and why?

10. Under what circumstances is deidentified, ''anonymized,'' or

[17] *Data Brokers: A Call for Transparency and Accountability* at i–v, Federal Trade Commission (May 2014), *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[18] *Data Brokers: A Call for Transparency and Accountability* at app. B, Federal Trade Commission (May 2014), *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[19] *See, e.g.,* 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), *https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.*

[20] *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* Pew Research Center (Nov. 2019), *https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.*

aggregated data reidentified or disaggregated?

11. Can people reasonably avoid adverse consequences resulting from data collection across different contexts (*e.g.,* cross-device tracking, re-identification, mobile fingerprint matching)?

12. Which specific entities and types of entities purchase data from data brokers? How do these entities use the purchased data?

a. What specific uses concern marketing, decisioning, fraud detection, or servicing related to consumer financial products and services?

b. What, if any, restrictions do data brokers impose on the use of such data?

13. What data broker practices cause harms to people? What are those harms and types of harms?

a. Are there certain special populations that are more likely to experience harms? If so, which special populations and why?

b. Are data brokers selling, reselling, or licensing information about particular groups, including certain protected classes? If so, what are examples of this behavior?

c. What harms do people experience if they are unable to remove their information from data broker repositories?

14. What data broker practices provide benefits to people? What are those benefits?

15. What actions can people take to gain knowledge or control over data, or correct data that is collected, aggregated, sold, resold, licensed, or otherwise shared about them?

16. How can and does the activity of data brokers and their clients impact consumers beyond those whose data were collected or used by that data broker? How, if at all, can consumers reasonably avoid being targeted or influenced based on the activities of data brokers and their clients, even if they are able to avoid or opt-out of having their own data collected?

17. What information do State-level data broker registries provide? How is this information made available and used? Are State-level data broker registries adequate to prevent harm? How could they be improved?

18. What controls do data brokers implement in order to protect people's data and safeguard the privacy and security of the public? Are these controls adequate?

a. What controls exist related to who can purchase or obtain information from data brokers?

b. Are these controls adequate?

19. What controls do data brokers implement to ensure the quality and accuracy of data they have collected?

a. What controls exist related to ensuring the quality and accuracy of public records data, including court records?

b. Are these controls adequate?

20. How have data broker practices evolved due to new technological developments, including machine learning or other advanced computational methods?

21. Are there companies or other entities that help consumers understand and manage their relationship to, and rights with respect to, data brokers? If not, why not? What factors could further help such consumer-assisting companies and entities?

22. How might the CFPB use its supervision, enforcement, research, rulemaking, or consumer complaint functions with respect to data brokers and related harms?

Individual Inquiries

1. Have you experienced data broker harms, including financial harms? What are those harms?

2. Have you experienced data broker benefits? What are those benefits?

3. Are you able to detect whether harms or benefits are tied to a specific data broker? Are existing methods of detection adequate?

4. Have you ever attempted to remove your data from a specific data broker's repository for privacy purposes? If so,

a. Describe your experience engaging with the data broker in question.

b. What steps were you required to take to request the removal of your data? Did you face any hurdles in filing the data removal request? Did the data broker honor your request?

c. Was your information removed immediately, and if not, how long did the removal take?

d. Were you asked to share additional information with the data broker to have your data removed?

e. Were you charged a fee by the data broker to have your data removed?

f. Did you spend money on another service to help you get your data removed? Was it helpful?

g. If your data removal request was successful, did you receive advertising to remove your data from other sites?

h. When you found your information on data broker websites, how did that make you feel?

5. Have you ever attempted to view or inspect the data maintained about you? If so, describe your experience.

a. What steps were you required to take to view or inspect your data?

b. Did you face any hurdles in filing the request to view or inspect your data?

c. Did the data broker honor your request?

6. Have you ever attempted to correct your data? If so, describe your experience.

a. What steps were you required to take to request correcting your data?

b. Did you face any hurdles in filing the data correction request?

c. Did the data broker honor your request?

7. Have you taken any other steps to protect your privacy or security as a result of data broker harms? Were these steps adequate?

Rohit Chopra,

Director, Consumer Financial Protection Bureau.

[FR Doc. 2023–05670 Filed 3–20–23; 8:45 am]

BILLING CODE 4810–AM–P

BUREAU OF CONSUMER FINANCIAL PROTECTION

[Docket No. CFPB–2023–0022]

Agency Information Collection Activities: Comment Request

AGENCY: Bureau of Consumer Financial Protection.

ACTION: Notice and request for comment.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995 (PRA), the Consumer Financial Protection Bureau (Bureau or CFPB) requests the extension of the Office of Management and Budget's (OMB's) approval of an existing information collection titled ''Truth in Lending Act (Regulation Z)'' approved under OMB Number 3170–0015.

DATES: Written comments are encouraged and must be received on or before April 20, 2023 to be assured of consideration.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain*. Find this particular information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function. In general, all comments received will become public records, including any personal information provided. Sensitive personal information, such as account numbers or Social Security numbers, should not be included.

FOR FURTHER INFORMATION CONTACT: Requests for additional information should be directed to Anthony May, Paperwork Reduction Act Officer, at (202) 435–7278, or email: *CFPB_PRA@cfpb.gov*. If you require this document in an alternative electronic format,