epic.org

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

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CONSUMER FINANCIAL PROTECTION BUREAU

On the Required Rulemaking on Personal Financial Data Rights

88 Fed. Reg. 74,796

December 22, 2023

I. Introduction

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Consumer Financial Protection Bureau (CFPB or the Bureau)'s Notice of Proposed Rulemaking (NPRM) on Personal Financial Data Rights, published on October 19, 2023.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has long advocated for privacy rights, robust data security safeguards, data minimization, and algorithmic accountability to protect consumers.[3]

[1] CFPB, *Notice of Proposed Rulemaking on Personal Financial Data Rights*, CFPB-2023-0052 (Oct. 19, 2023) [hereinafter "*PFDR NPRM*"].
[2] *About Us*, EPIC, https://epic.org/about/ (2023).
[3] *See* EPIC, *In re Rocket Money* (Dec. 2022), https://epic.org/documents/epic-cfpb-complaint-rocket-money/; EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, FTC Commercial Surveillance ANPRM, R111004 (Nov. 2022), https://epic.org/wpcontent/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; Consumer Reports and EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wpcontent/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; EPIC Statement to U.S. House Committee on House Administration, Hearing on "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" (Feb. 16, 2022), https://epic.org/documents/hearing-onbig-data-privacy-risks-and-needed-reforms-in-the-public-and-private-sectors/; EPIC Comments on CFPB Inquiry Into Big Tech Payment Platforms, CFPB-2021-0017 (Dec. 2021),

EPIC urges the CFPB to promulgate rules that will empower consumers in their interactions with the financial services industry. The final rule should facilitate frictionless access by consumers to their financial information, enable consumers to understand and control who has access to their personal information and for what purposes they may use it, and prohibit third parties from collecting, using, or retaining personal information beyond what is reasonably necessary to provide the product or service requested by the consumer.[4]

EPIC supports the CFPB's efforts to safeguard consumer data rights in the financial services industry. EPIC has previously engaged with the Bureau's work on this issue through our January 2023 comments in response to the Bureau's Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights.[5] We commend the Bureau for proposing rules that will strengthen protections for consumers in the financial services industry. This comment recommends several refinements to the CFPB's proposals. It is organized into the following topics: data minimization, ongoing use and retention of data, consumer rights, account verification, data security, and qualified industry standards.

II. Data Minimization

EPIC has long advocated for the inclusion of data minimization principles in regulation, including in a 2022 white paper co-authored by Consumer Reports,[6] in comments to the Federal

---

https://epic.org/documents/epiccomments-on-cfpb-inquiry-into-big-tech-payment-platforms/; EPIC, Comments on CFPB Request for Information on the Equal Credit Opportunity Act and Regulation B, 85 Fed. Reg. 46,600 (Oct. 2, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CFPB-Oct2020-AI-ML.pdf. *See generally* EPIC, *Data Brokers* (2023), https://epic.org/issues/consumer-privacy/data-brokers/.

[4] *See* EPIC, Comments on Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights(Jan. (Jan. 25, 2023), https://epic.org/wp-content/uploads/2023/01/EPIC-Comment-CFPB-Financial-Data-Rights-Rulemaking-Jan2023.pdf [hereinafter "PFDR SBREFA Comment"]; 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).

[5] *PFDR SBREFA Comment*.

[6] EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://epic.org/wpcontent/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

Trade Commission concerning the FTC's rulemaking on commercial surveillance and data security,[7] and in our previous comments to the CFPB.[8] Data minimization is the most effective tool for protecting consumer privacy, adhering commercial data practices to consumer expectations, and safeguarding personal information.

We commend the Bureau for proposing restrictions on third party collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service.[9] The proposed rule rightly incorporates data minimization principles to provide strong privacy protections for consumers. But to further strengthen this standard, EPIC recommends that the Bureau require third parties to collect, use, and retain covered data only when doing so is consistent with the reasonable expectations of the consumer. Specifically, we propose amending § 1033.421(a)(1) to read (proposed edits in red):

> The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service **and consistent with the reasonable expectations of the consumer**.

Limiting third party data collection, use, and retention according to the reasonable expectations of the consumer is critical to an effective data minimization protocol. Incorporating this framework will ensure that the final rule does not place the burden on consumers to protect their own privacy by policing the privacy policies and practices of the financial products and services they use.[10] We recommend that the Bureau look to the California Consumer Protection Act (CCPA) regulations,

---

[7] EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, Commercial Surveillance ANPR, R111004 (Nov. 2022), https://epic.org/documents/disruptingdata-abuse-protecting-consumers-from-commercial-surveillance-in-the-online-ecosystem/.

[8] *PFDR SBREFA*; EPIC, Comments on the Small Business Advisory Review Panel for Consumer Reporting Rulemaking (Oct. 30, 2023), https://epic.org/wp-content/uploads/2023/10/EPIC-CFPB-FCRA-SBREFA-Comment.pdf.

[9] *PFDR NPRM*, § 1033.421(a)(1).

[10] Suzanne Bernstein, *Data Minimization: Centering Reasonable Consumer Expectations in the FTC's Commercial Surveillance Rulemaking*, EPIC (Apr. 20, 2023), https://epic.org/data-minimization-centering-reasonable-consumer-expectation-in-the-ftcs-commercial-surveillance-rulemaking/.

which are instructive for properly framing a reasonable consumer expectation standard. To determine the reasonable expectation of the consumer, the regulations set out five factors: (1) the relationship between the consumer and the business; (2) the nature of the personal information that a business seeks to collect or process; (3) the source of the personal information and method for collection or processing; (4) the "specificity, explicitness, prominence, and clarify of disclosures to the consumer"; and (5) the degree to which the involvement of contractors, service providers or third parties are apparent to the consumer.[11] Incorporating a reasonable expectation of the consumer standard into the final rule will prevent entities from extracting nominal "consent" for unrestricted collection, use, and retention of personal data. Instead, a final rule that incorporates this standard would protect consumers' reasonable expectation that their personal data will be processed by the entities they have entrusted it to only to the extent necessary to provide the products and services consumers have requested.[12]

We commend the Bureau for including limits on secondary uses of covered data in the proposed rule. The proposed rule only permits use of covered data when it is reasonably necessary and specifically states that targeted advertising, cross-selling of other products or services, and the sale of covered data are not reasonably necessary to provide any products or services. We recommend including clear and specific definitions and examples of targeted advertising,[13] cross-

[11] Cal. Code Regs. tit. 11 § 7002.
[12] Bernstein, *supra* note 10.
[13] We recommend that the Bureau look to the definition of targeted advertising set forth in the State Data Privacy and Protection Act § 2(a)(35), https://epic.org/wp-content/uploads/2023/02/State-Privacy-Act-bill-text.pdf (defining "targeted advertising" as presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier; provided, however that "targeted advertising" does not include: advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback; contextual advertising, which is when an advertisement is displayed based on the content or nature of the website or service in which the advertisement appears and does not vary based on who is viewing the advertisement; or processing covered data strictly necessary for the sole purpose

selling of other products or services, and sale of covered data[14] within section 1033.421(a)(2) of the rule. Providing definitions for these terms would enhance clarity of the rule by specifically stating which behaviors are not reasonably necessary.

Additionally, we recommend that the Bureau specify that behavioral profiling—using a consumer's personal data to make inferences about the consumer's future behavior[15]—is presumptively not reasonably necessary to provide products or services. Behavioral profiling may be acceptable when it is actually essential to providing the consumer's requested product or service; for example, detecting fraud or providing credit offers specifically sought by the consumer may be acceptable uses of behavioral profiling. However, many other types of behavioral profiling—such as profiling for secondary commercial purposes—are not reasonably necessary to provide a consumer's requested product or service and should be prohibited.

The rule should also provide enhanced restrictions on the collection, use, and retention of sensitive personal information. Most categories of personal data would be appropriately protected by the reasonable necessity and reasonable expectation standards, but sensitive personal information poses a greater risk of harm to consumers if exposed or misused. Therefore, the Bureau should limit third parties' collection, use, and retention of sensitive personal information to what is *strictly* necessary to provide the product or service the consumer requests, and only consistent with the reasonable expectations of the consumer. To facilitate these heightened restrictions, the CFPB

---

of measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement).

[14] We recommend that the Bureau look to the CCPA's definition of "sale" provided in Cal. Code Regs. tit. 1.81.5, § 1798.140(ad).

[15] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Art. 4(4) (defining "profiling" as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements).

should also adopt a definition of "sensitive personal information" that sets out a non-exhaustive list of sensitive data types. We recommend that the Bureau look to the State Data Privacy and Protection Act's definition of sensitive covered data as a basis for this list.[16]

III. Ongoing Use and Retention of Data

Financial services companies advertise a wide variety of products and services used for investing, budgeting, and spending to consumers. These companies frequently do not charge for their products and services, but instead collect an immense amount of personal data about consumers. Given the complexity and opacity surrounding data collection, use, retention, and dissemination by providers of financial products and services, it is difficult for consumers to understand and keep track of which entities have continuing access to their data. It is therefore vital to establish robust data protection rules, especially given the sensitivity of personal financial data.

To this end, EPIC commends the CFPB's proposed rules regarding regular disclosures to consumers, limits on third party access to consumer data, and the reauthorization process for third party access to consumer data. However, we recommend strengthening the proposed rule's data deletion provisions. Currently, the proposed rule permits third parties to retain consumer data as long as it is reasonably necessary to provide the consumer's requested product or service.[17] We recommend providing a presumptive, affirmative data deletion deadline in the proposed rule. Third parties should be affirmatively required to delete consumer data which has not been used in connection with the provision of products or services requested by the consumer for over three years unless the consumer data must be retained to comply with other laws.[18] Further, the Bureau should require data retention beyond three years to be supported by documentation that the data continues to

[16] § 2(30), https://epic.org/wp-content/uploads/2023/02/State-Privacy-Act-bill-text.pdf.
[17] *PFDR NPRM*, § 1033.421(a)(1).
[18] *See In re Global Tel*Link, TelMate, and TouchPay Holdings*, FTC File No. 212-3012 (Nov. 16, 2023) (consent order).

be reasonably necessary for the provision of the consumer's requested products or services. Notably, relying on a three-year deadline would harmonize the deletion requirement with the proposed rule's three-year data retention requirement.[19] Financial entities need not—and should not—retain consumer data indefinitely once a consumer is no longer using the product or service, and lengthy retention of personal data increases the risk that a consumer's data may be breached or improperly used for another purpose.

IV. Consumer Rights

EPIC applauds the Bureau for proposing rules establishing and solidifying consumers' rights respecting their personal data. It is important (though not sufficient, as the Bureau knows) for data providers to disclose key information to consumers, and of course consumers should be empowered with control over their own data. This section proposes refinements to the rules regarding disclosures and revocation of third-party authorization to access consumer data.

We commend the Bureau for proposing rules that would require data providers to disclose important information to consumers. Providing information to consumers about how their data is collected, used, shared, and retained empowers consumers to make more meaningful decisions about which financial products and services they use and to take steps to protect the security of their own data. However, the responsibility to protect data privacy and security should not be placed on consumers alone, particularly because there is often a power imbalance between businesses and consumers, and there may be circumstances where consumers lack meaningful alternatives to companies whose data practices they do not like. This makes the meaningful obligations the proposed rule places on data providers and its restrictions on third parties' access to consumer data even more critical. However, we offer three recommendations to strengthen the existing language.

[19] *PFDR NPRM*, § 1033.351(d)(1).

First, as we noted in our comment at the SPREFA stage,[20] the rules should clarify how data providers may verify consumers' identities when consumers request access to information in § 1033.331(a)(1). Because of the sensitive nature of the data that entities may collect to verify consumers' identities, we urge the CFPB to only permit data collection for identity verification purposes if doing so is strictly necessary and to integrate purpose specification into the required disclosures. If data is collected for multiple purposes, data providers should be required to specify all purposes for collection to allow consumers to approve of each purpose.

Second, the Bureau should narrow the scope of statutory exceptions in § 1033.331(c) to making information available to consumers. Consumers deserve transparency about the financial products and services they use, so the final rule should permit fewer exceptions to the requirement that data providers make information available to consumers. The CFPB should narrowly define the scope of "confidential commercial information" included in § 1033.221(a). The rule should clarify that consumers have a right to know when a data provider is using an algorithm to derive credit scores, risk scores, or make other predictions. Further, the Bureau should narrow the scope of § 1033.221(d), which provides that "Any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information." Failing to define "ordinary course of business" may allow data providers to find loopholes or shield themselves from disclosing information that they should be required to provide to consumers.

Third, the Bureau should strengthen the proposed rule provisions pertaining to a consumer's power to revoke third-party authorization to access the consumer's data. Currently, § 1033.331(e) permits data providers to provide consumers a reasonable method to revoke any third party's authorization to access the consumer's data. We propose that the Bureau promulgate a rule that

[20] *PFDR SBREFA Comment* at 7.

requires rather than *permits* data providers to provide a reasonable revocation method to consumers. Consumers deserve autonomy over their own data, and it is essential to provide easy methods for consumers to revoke third parties' authorization to access their data from both the provider side and the third-party side. We understand that some entities may have competition concerns arising from the availability of a provider-side data access revocation method to consumers. While the Bureau can and should use other rules and oversight mechanisms to address these concerns, it is essential to require data providers to provide a reasonable third-party data access revocation method to consumers to protect individual data autonomy and help consumers protect themselves from harmful data breaches.

V. Account Verification

Robust account verification procedures are necessary to protect consumers from unauthorized account access by data brokers, hackers, private investigators, and other entities.[21] We applaud the CFPB for requiring strong account verification procedures to prevent privacy harms, data breaches, and fraud. In particular, we support the robust requirements for data providers to verify a third party's authorization to access consumer data and authenticate the identity of third parties before they access consumer data.[22]

We also commend that proposed rule's requirement that third parties comply with the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework or the FTC Standards for Safeguarding Customer Information.[23] These rules include important provisions related to account verification,

[21] *See* FCC Proposes Over $200M in Fines for Wireless Location Data Violations (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations; *Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"*, Krebs on Security (Mar. 29, 2022), https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergencydata-requests/; William Turnton, *Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests*, Bloomberg (updated March 30, 2022, 3:30 PM), https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests.
[22] *PFDR NPRM*, § 1033.321(d).
[23] 16 C.F.R. § 314.

such as requiring additional verification methods such as multi-factor authentication when consumers attempt to access their account information.

We recommend that the CFPB also include provisions in the proposed rule that would require data providers to establish procedures to verify the validity of data access requests that appear to result from lawful process. Consumer protection agencies consistently encourage consumers who may be the target of attempted government impersonation fraud to hang up the phone or ignore fraudulent texts and emails, go to the agency's .gov website, and use the contact information provided on the .gov website to seek clarification.[24] Companies that have access to consumer financial data should at least be held to this standard when responding to apparent government requests for access to consumer data. Procedures for verifying the validity of government access requests should always be followed, even when an entity receives an emergency government access request.[25] Establishing such procedures would help to protect consumers from fraudulent data access requests, including government impersonation fraud.[26]

[24] *See, e.g.*, *Fraud Alert – May 5, 2022*, State of California Department of Consumer Affairs, https://www.dca.ca.gov/licensees/scam_alert.shtml (last accessed Jan. 24, 2023); *SCAM ALERT: LA County Will Not Ask For your Info In Unexpected Phone Calls*, Los Angeles County Department of Consumer & Business Affairs (Feb. 11, 2022), https://dcba.lacounty.gov/newsroom/scam-alert-la-county-phone-spoofingscam/; FTC Consumer Advice, *How to Avoid a Government Impersonator Scam*, https://consumer.ftc.gov/articles/how-avoid-government-impersonator-scam (last accessed Jan. 24, 2023).
[25] *See, e.g.*, *DEA Investigating Breach of Law Enforcement Data Portal*, Krebs on Security (May 12, 2022), https://krebsonsecurity.com/2022/05/dea-investigating-breach-of-law-enforcement-data-portal/ (noting in the context of a DOJ database being hacked that "when hackers can plunder 16 law enforcement databases, arbitrarily send out law enforcement alerts for specific people or vehicles, or potentially disrupt ongoing law enforcement operations — all because someone stole, found or bought a username and password — it's time for drastic measures.").
[26] *Id*.

VI. Data Security

EPIC applauds the CFPB for including strong data security protections in the proposed rule. Data breaches and identity theft severely harm consumers,[27] and companies must be required to invest in data security.

We commend the Bureau for requiring GLBA-covered financial institutions to comply with the GLBA Safeguards Framework and requiring other entities to comply with the FTC's Safeguards Rule for the implementation of developer interfaces, interface access, and third-party access to consumer data. Companies should be required to maintain data security standards commensurate with the scope and scale of the data collected.[28] As we noted in our SBREFA comment, it is essential to require financial services entities to implement data security procedures including, but not limited to, access controls, secure password practices, user authentication, system segmentation, traffic monitoring, staying current on known vulnerabilities, security reviews, and employee training.[29] The GLBA Safeguards Framework and FTC Safeguards Rule incorporate these requirements, so the rules provide strong data security protections for consumers in the financial services industry.

To strengthen data security protections for consumers, we recommend that the Bureau clearly state in the final rule that third parties are liable to consumers if consumer credentials are

---

[27] *See, e.g.*, Verizon, *Financial Services Data Breaches*, https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financialservices-data-breaches/ (last accessed Jan. 24, 2022); Paul Bischoff, *Financial data breaches accounted for 153.3 million leaked records from January 2018 to June 2022*, Comparitech (updated July 27, 2022), https://www.comparitech.com/blog/vpn-privacy/financial-data-breaches/.

[28] *See, e.g.*, William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1179 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf (noting that across multiple data security frameworks "the duty of data security scales up or down in proportion to the resources and risk profile of each data custodian").

[29] *PFDR SBREFA Comment* at 17; *See* EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, FTC Commercial Surveillance ANPRM, R111004 (Nov. 2022), https://epic.org/wpcontent/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; *See, e.g.*, William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1179 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf (at 199, 201–05).

compromised from their systems. Assigning liability to third parties for breaches of consumer credentials on their system will ensure that third parties are incentivized to implement strong data security protections as required by the rule.

VII. Qualified Industry Standards

We commend the Bureau for establishing detailed requirements for the development of qualified industry standards, which are used throughout the rule to evaluate the sufficiency of developer interfaces, disclosures to consumers, and consumer revocation and data access authorization methods. In particular, we applaud the CFPB for highlighting that the industry standards must balance the needs of all parties, including consumer and public interest groups, at all levels of the standard setting body.[30] Prioritizing balance will help to ensure that consumers and public interest advocates will have a seat at the table while standards are developed. In relation to the "openness" attribute,[31] we urge the CFPB to specify that all working groups, subcommittees, and other subordinate units of standard setting bodies must also conduct their proceedings openly and transparently. Absent this clarification, there is a risk that standards setting bodies will resort to closed-door subgroup meetings to conceal the content and participants of the deliberations that yield proposed standards.[32]

Additionally, we encourage the Bureau to ensure that the timeline for development of qualified industry standards is synchronized with the timeline for compliance with the final rule. For example, data providers must comply with the rule between six months and four years after the rule

[30] *PFDR NPRM*, § 1033.141(a)(2).
[31] *PFDR NPRM*, § 1033.141(a)(1).
[32] *Cf.* EPIC, *EPIC v. Drone Advisory Committee* (2021) ("[T]he DAC established a DAC Subcommittee to 'conduct more detailed business' than would typically be addressed by the full committee. The DAC also established three 'Task Groups' to address specific drone-related issues . . . . Yet none of the DAC Subcommittee or Task Group meetings were open to the public, and very few records documenting their proceedings have been released.").

is published in the Federal Register.[33] Therefore, the Bureau should ensure that qualified industry standards can be thoughtfully developed within six months of the finalization of the rule so that covered entities can rely on the qualified industry standards when they must come into compliance with the rule.

VIII. Conclusion

We applaud the Bureau's work to establish stronger privacy and data security protections for consumers in the financial services industry while encouraging competition in the financial services market. EPIC appreciates the opportunity to provide recommendations and feedback on the proposed rule. We are eager to engage further with the Bureau as the rule is finalized. If you have any questions, please don't hesitate to reach out to EPIC Law Fellow Caroline Kraczon, (kraczon@epic.org).

Respectfully submitted,

/s/ John Davisson
John Davisson
Director of Litigation

/s/ Caroline Kraczon
Caroline Kraczon
Law Fellow

[33] *PFDR NPRM*, § 1033.121.