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 Advanced Notice of Public Rulemaking on Personal Financial Data Rights Reconsideration

Docket No. CFPB-2025-0037

October 21, 2025

---

## I. Introduction

The Electronic Privacy Information Center (EPIC) and the undersigned consumer protection, digital justice, and privacy organizations submit these comments in response to the Consumer Financial Protection Bureau (CFPB or the Bureau)'s Advanced Notice of Proposed Rulemaking (NPRM) on Personal Financial Data Rights Reconsideration, published on August 22, 2025.[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, and data minimization standards to protect consumers, including in the financial sector.[3]

---

[1] CFPB, *Advanced Notice of Proposed Rulemaking on Personal Financial Data Rights Reconsideration*, CFPB-2025-0037 (Aug. 22, 2025).
[2] *About Us*, EPIC, https://epic.org/about/ (2023).
[3] *See, e.g.* EPIC, Comments on Notice of Proposed Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74,796 (Dec. 22, 2023), https://epic.org/documents/comments-of-epic-to-the-cfpb-on-the-required-rulemaking-on-personal-financial-data-rights/ [hereinafter "EPIC PFDR NPRM Comment"]; *EPIC Joins NCLC to Urge the CFPB to Protect Consumer Financial Privacy*, EPIC (Apr. 16, 2025), https://epic.org/epic-joins-nclc-to-urge-the-cfpb-toprotect-consumer-financial-privacy/; Caroline Kraczon and Justin Sherman, *Unbridled and Underregulated: Removing FCRA and GLBA Exemptions from Privacy Laws to Hold Data*

We urge the CFPB to maintain the strong consumer rights and data privacy and security standards that the Bureau included in the Personal Financial Data Rights (PFDR) rules finalized in October 2024.[4] The data access and portability provisions included in the PFDR rules gave consumers autonomy over their personal financial information, facilitating frictionless access by consumers to their own financial information. Similar data access and portability provisions included in state privacy laws have garnered broad bipartisan support. The finalized rules also included some of the strongest privacy and data security protections in federal law, empowering consumers to understand and control who has access to their financial information and for which purposes they may use it.

The robust privacy and data security standards included in the PFDR rules are both critical and appropriate, as personal financial information is particularly sensitive data. If financial information is breached, fraudsters and scammers may gain access, resulting in potentially devastating financial losses for victims. For example, fraudsters may use personal financial data to target victims for scams. Financial data can also be used to give a false air of credibility to fraud

---

*Brokers Accountable*, EPIC (July 2025); EPIC, NCL, and CFA, *Comments on the Protecting Americans from Harmful Data Broker Practices Notice of Proposed Rulemaking*, CFPB-2024-0044 (April 2025), https://epic.org/documents/comments-of-epic-ncl-and-cfa-on-the-protecting-americans-from-harmful-data-broker-practices-notice-of-proposed-rulemaking/; *PRESS RELEASE: EPIC and Americans for Financial Reform Oppose Attempt to Strip Away Payment App Protections*, EPIC (Mar. 10, 2025), https://epic.org/press-release-epicand-americans-for-financial-reform-oppose-attempt-to-strip-away-payment-app-protections/; *EPIC Executive Director Testifies Before the House Financial Services Committee*, EPIC (Dec. 4, 2024), https://epic.org/epicexecutive-director-testifies-before-the-house-financial-services-committee/; *EPIC Submits Comments to Strengthen CFPB Proposals for Financial Data Rights Rulemaking* (Jan. 25, 2023), https://epic.org/epicsubmits-comments-to-strengthen-cfpb-proposals-for-financial-data-rights-rulemaking/; 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. *See generally* EPIC, *Data Brokers* (2025), https://epic.org/issues/consumer-privacy/data-brokers/.

[4] CFPB, *Final Rule – Required Rulemaking on Personal Financial Data Rights*, CFPB-2023-0052 (Nov. 18, 2024), https://www.federalregister.gov/documents/2024/11/18/2024-25079/required-rulemaking-on-personal-financial-data-rights [hereinafter "PFDR Final Rule"].

schemes.[5] If a fraudster contacts an individual claiming to be a representative from the individual's bank, the person is more likely to fall for the scheme if the fraudster provides accurate information related to the individual's bank account.[6] A report by the Federal Trade Commission estimated that consumers lost over $158 billion to fraud in 2023 alone.[7] The Bureau must ensure that financial institutions follow strong privacy and data security standards to ensure that consumers' financial information is not exposed to fraudsters and scammers.

Protecting the security of financial information is also critical for national security. If information held by financial institutions is exposed during a data breach, criminals and foreign adversaries may be able access and use the information in ways that put our country at risk. The data broker industry accelerates harm caused by data breaches because the information held by data brokers may include financial information exposed in a data breach. Data brokers compile and sell detailed profiles about individuals, often without using sufficient security controls to prevent the data from reaching malicious actors. 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.[8] Further, 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

[5] *Phishing Scams*, American Bankers Association, https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/phishing (last visited Sept. 16, 2025).
[6] *Id*.
[7] *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.
[8] 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/.

brokers use to target online advertisements.[9] Bad actors can use sensitive financial information purchased from data brokers to carry out blackmail or facilitate phishing tactics to obtain state secrets from military and government personnel.[10]

As the Bureau considers the PFDR rule for a second time, it must ensure that financial institutions keep consumers' financial information private and secure while empowering consumers to access and control their own financial data held by financial institutions. The PFDR rules accomplished these goals, and we urge the CFPB to preserve them as is.

## II. Privacy and Data Security

The PFDR rules finalized by the CFPB in October 2024 included robust privacy and data security requirements for third parties authorized by a consumer to access personal financial information, including data minimization obligations, limits on secondary uses of personal data, and data security standards. Privacy and data security protections go hand in hand. Limiting third parties' ability to collect, share, and use personal information both protects consumer privacy and decreases the likelihood of data breach or misuse; you do not have to protect the security of data that you do not collect in the first place. As detailed in the previous section, financial information is a particularly sensitive category of information. As the Bureau reconsiders the PFDR rules, we urge the Bureau to preserve the strong data privacy and security rules that are included in the existing rules.

---

[9] 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 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.

[10] *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/.

*This subsection is responsive to Question 18: Does the PFDR Rule provide adequate protections for the security of consumer's data? Why or why not?*

Yes, the PFDR rule provides adequate data security protections for consumer data. The PFDR rule includes robust data security protections that must be preserved as the committee reconsiders the rule. Data breaches and identity theft severely harm consumers,[11] and companies must be required to invest in data security. We support the PFDR rule's requirement that third parties comply with the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework or the FTC Standards for Safeguarding Customer Information.[12] These frameworks include robust provisions related to data security and account verification and data security, so we recommend maintaining the requirement that institutions comply with these frameworks. Companies should be required to maintain data security standards commensurate with the scope and scale of the data collected.[13] For example, financial services entities must 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.[14] The GLBA Safeguards Framework and FTC Safeguards Rule incorporate these

[11] *See, e.g.*, Verizon, *2025 Data Breach Investigation Report*, https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financialservices-data-breaches/ (last accessed Sept. 26, 2025); Paul Bischoff, *Financial data breaches accounted for 232 million leaked records across 2260 data breaches*, Comparitech (updated Oct. 4, 2023), https://www.comparitech.com/blog/vpn-privacy/financial-data-breaches/.
[12] 16 C.F.R. § 314.
[13] 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").
[14] *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.

requirements, providing strong data security protections for consumers in the financial services industry.

The PFDR rules provide adequate data security protections for consumers, and if the Bureau wishes to strengthen the data security provisions even further, we recommend the two following additional provisions.

First, we recommend that the CFPB also include provisions in the PFDR 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.[15] 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.[16] Establishing such procedures would help to protect consumers from fraudulent data access requests, including government impersonation fraud.[17]

---

[15] *See, e.g.*, *Scam Alerts*, State of California Department of Consumer Affairs, https://www.dca.ca.gov/licensees/scam_alert.shtml (last accessed Sept. 26, 2025); *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 Sept. 26, 2025).

[16] *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.").

[17] *Id*.

Second, we recommend that the Bureau add a provision to the PFDR rules clearly stating that third parties are liable to consumers if consumer credentials are 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.

*This subsection is responsive to Question 27: To what information security standards ought entities adhere when accessing consumer financial data held by a covered person, and who is best positioned to evaluate whether these entities are adhering to such standards?*

As discussed above in response to Question 18, The GLBA Safeguards Framework or FTC Standards for Safeguarding Customer Information provide sufficient information security standards to ensure that entities fulfill the data security requirements of the PFDR rule. Further, federal financial regulators at CFPB and FTC should be empowered to monitor compliance and enforce against violations.

*This subsection is responsive to Question 29: Does the PFDR Rule provide adequate protections for consumers and covered persons to ensure that the request for a consumer's information is in fact knowingly authorized by the individual consumer and that the information is in fact being made available to the consumer as opposed to a malicious actor?*

Yes, the PFDR rules include strong account verification requirements, which ensure that data providers verify the identity of consumers and their authorized representatives. These rules are necessary to protect consumers from unauthorized account access by hackers, data brokers, private investigators, and other entities.[18] Section 1033.321 includes robust requirements for data providers

[18] *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),

to verify a third party's authorization to access consumer data and authenticate the identity of third parties before they access consumer data.[19] Further, the rule's requirement that third parties comply with the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework or the FTC Standards for Safeguarding Customer Information also helps to ensure that information is not provided to unauthorized persons or malicious actors.[20] These rules include important provisions related to account verification, including requiring additional verification methods such as multi-factor authentication when consumers attempt to access their account information. We recommend that the CFPB maintain the strong account verification provisions included in the PFDR rules.

*This subsection is responsive to Question 30: Does the PFDR Rule provide adequate protection of consumer privacy? Why or why not?*

Yes, the PFDR rule includes strong privacy provisions that provide sufficient protection for consumers, so we recommend that the CFPB maintain those privacy protections as it reconsiders the PFDR rule. The PFDR rules include a strong data minimization standard that must be maintained as the CFPB reconsiders the rule. EPIC has long advocated for the inclusion of data minimization principles in regulation, including in a 2022 white paper co-authored by Consumer Reports,[21] in comments to the Federal Trade Commission concerning the FTC's rulemaking on commercial

---

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.

[19] *PFDR Final Rule*, § 1033.321(d).

[20] 16 C.F.R. § 314.

[21] 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_0.

surveillance and data security,[22] and in our previous comments to the CFPB.[23] Data minimization is the most effective tool for protecting consumer privacy, adhering commercial data practices to consumer expectations, and safeguarding personal information. The rule rightly incorporates data minimization principles to provide strong privacy protections for consumers by restricting third parties' collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service.

To strengthen the data minimization provisions of the PFDR rule even further, we recommend 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 bolded):

> 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 would 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.[24] Incorporating a reasonable expectation of the consumer standard into the final rule would prevent entities from extracting nominal "consent" for unrestricted collection, use, and retention of personal data. Instead, a PFDR rule that

---

[22] 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/.

[23] *EPIC PFDR NPRM Comments*; 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.

[24] 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/.

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.[25]

We also support the PFDR rule's limits on secondary uses of covered data. The 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. To further strengthen this portion of the PFDR rule, we recommend including clear and specific definitions and examples of targeted advertising,[26] cross-selling of other products or services, and sale of covered data[27] 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.

Further, the PFDR rules include strong provisions relating to the 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

---

[25] *Id*.

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

[27] 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).

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. To this end, the PFDR rule includes provisions regarding regular disclosures to consumers, limits on third party access to consumer data, and the reauthorization process for third party access to consumer data.

The PFDR rule permits third parties to retain consumer data as long as it is reasonably necessary to provide the consumer's requested product or service.[28] To strengthen the rule, we recommend providing a presumptive, affirmative data deletion deadline in the PFDR 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.[29] Further, the Bureau should require data retention beyond three years to be supported by documentation that the data continues to 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 rule's three-year data retention requirement.[30] 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.

## III. Proper Understanding of a "Representative" Making a Request on Behalf of the Consumer

The Bureau must ensure that consumers can exercise their rights granted within the PFDR rule with ease. The Dodd-Frank Act empowers consumers to utilize an agent, trustee, or

[28] *PFDR Final Rule*, § 1033.421(a)(1).
[29] *See In re Global Tel*Link, TelMate, and TouchPay Holdings*, FTC File No. 212-3012 (Nov. 16, 2023) (consent order).
[30] *PFDR Final Rule*, § 1033.351(d)(1).

representative to act on their behalf when exercising their rights under Dodd-Frank. This mechanism is important because it allows consumers to easily exercise their rights. While considering the proper interpretation of the term "representative," the CFPB must take care not to limit consumers' right to use an authorized representative to exercise rights on their behalf.

Colorado and California have both promulgated rules pursuant to their state privacy laws that include provisions focusing on requirements for and authentication of authorized agents acting on behalf of consumers to exercise their privacy rights. Both states provide strong provisions to ensure that authorized agents or representatives are who they say they are and actually have permission from the consumer to act on their behalf. We recommend that the CFPB look to the rules finalized in those states when determining who can serve as a "representative" for consumers, as well as how to authenticate consumers' representatives.

*Colorado*

The Colorado Privacy Act (CPA) Rules permit authorized agents to exercise a consumer's opt-out right on the consumer's behalf as long as the controller is able to authenticate the consumer's identity and the authority of the authorized agent to act on the consumer's behalf.[31] Rule 4.08 relates to authentication of consumers and authorized agents. It states that a controller shall use a commercially reasonable method for authenticating the identity of consumers submitting a Data Right request, and the authority of Authorized Agents submitting an opt-out request on behalf of a consumer.[32] When determining if an authentication method is commercially reasonable, the CPA rules direct controllers to consider following factors: "the Data Rights exercised, the type, sensitivity, value, and volume of Personal Data involved, the level of possible harm that improper access or use could cause to the Consumer submitting the Data Right request and the cost of

[31] 4 C.C.R. 904-3, Rule 4.03(C).
[32] 4 C.C.R. 904-3, Rule 4.08(A).

authentication to the Controller." The rules also state that a controller must avoid methods that place an unreasonable burden on consumers submitting Data Right requests or authorized agents submitting an opt-out requests on behalf of consumers.[33] Further, controllers may not charge a fee for the authentication of consumers or authorized agents or to require documentation that requires a fee; for example, controllers may not require a consumer to provide a notarized affidavit for authentication unless the controller reimburses the consumer for the cost of notarization.[34]

The CPA rules state that controllers shall implement reasonable security measures to protect personal information used to authenticate an authenticated agent, with consideration to the type, value, sensitivity, and volume of information and the level of possible harm that could be imposed on consumers if the information were improperly accessed. Rule 6.09(B) provides further consideration for controllers determining reasonable and appropriate safeguards, including "1. Applicable industry standards and frameworks; 2. The nature, size, and complexity of the Controller's organization; 3. The sensitivity and amount of Personal Data; 4. The original source of Personal Data; 5. The risk of harm to Consumers resulting from unauthorized or unlawful access, use, or degradation of the Personal Data; and 6. The burden or cost of safeguards to protect Personal Data from harm."[35]

Further, Rule 6.09(C) states that "reasonable and appropriate administrative, technical, organization, and physical safeguards must be designed to: 1. Protect against unauthorized or unlawful access to or use of Personal Data and the equipment used for the Processing and against accidental loss, destruction, or damage; 2. Ensure the confidentiality, integrity, and availability of Personal Data collected, stored, and Processed; 3. Identify and protect against reasonably anticipated

[33] 4 C.C.R. 904-3, Rule 4.08(A)(1).
[34] 4 C.C.R. 904-3, Rule 4.08(E).
[35] 4 C.C.R. 904-3, Rule 6.09(B).

threats to security or the integrity of information; and 4. Oversee compliance with data security policies by the Controller and Processors through reasonable requirements."[36]

*California*

Similarly, the California Consumer Privacy Act (CCPA) Regulations permit consumers to use an authorized agent to act on their behalf to exercise rights under the CCPA.[37] When a consumer uses an authorized agent to submit a request to a business to delete, correct, or to disclose information, the business may verify the authorized agent by requiring proof that the consumer gave signed permission to the authorized agent to submit a request on their behalf, require the consumer to verify their own identity, and require the consumer to directly confirm with the business that they gave an authorized agent permission to submit a request on their behalf.[38] California's rule impose certain data security and privacy requirements onto authorized agents. First, authorized agents must "implement and maintain reasonable security procedures and practices to protect the consumer's information."[39] Second, the authorized agent "shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention."[40]

## IV. Assessment of Fees in Response to a Customer Driven Request

We recommend that the Bureau preserve the prohibition against data providers imposing fees or charges on consumers or authorized third parties in connection with establishing or maintaining data access interfaces or providing covered data in response to requests.[41] Providing information to consumers about how their data is collected, used, shared, and retained empowers consumers to

[36] 4 C.C.R. 904-3, Rule 6.09(C).
[37] Cal. Code Regs. tit. 11 § 7001(d).
[38] Cal. Code Regs. tit. 11 § 7063(a).
[39] Cal. Code Regs. tit. 11 § 7063(c).
[40] Cal. Code Regs. tit. 11 § 7063(d).
[41] 12 CFR § 1033.301(c).

make more meaningful decisions about which financial products and services they use. The Bureau should maintain the previously finalized prohibition against data providers charging fees in response to consumer driven requests because the prohibition on fees both increases transparency and expands consumer autonomy over personal data.

## V. Conclusion

EPIC appreciates the opportunity to provide recommendations and feedback on consumer protections and privacy rights in the financial services sector. We are eager to engage further with the Bureau as the Personal Financial Data Rights Rule is reconsidered. If you have any questions, please reach out to EPIC Counsel Caroline Kraczon (kraczon@epic.org).

Respectfully submitted,

*/s/ John Davisson*
John Davisson
Director of Litigation
Electronic Privacy Information Center

*/s/ Caroline Kraczon*
Caroline Kraczon
Counsel
Electronic Privacy Information Center

Joined by:

Center for Democracy and Technology

Center for Digital Democracy

Check My Ads

Consumer Action

Consumer Federation of California

Demand Progress Education Fund

Privacy Rights Clearinghouse