Before the
Consumer Financial Protection Bureau
Washington, D.C.

In re Personal Financial Data Rights Reconsideration	Docket No. CFPB-2025-0037

COMMENTS OF

THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Advanced Notice of Proposed Rulemaking, published in the Federal Register at 90 Fed. Reg. 40986 (12 C.F.R. Part 1033), the Computer & Communications Industry Association ("CCIA")[1] submits the following comments.

I. Scope of Who May Make a Request on Behalf of a Consumer

Question 5: The term "representative" should be defined as any entity that provides a consumer with a financial product or service, and acts on behalf of the consumer in providing the financial product or service. The definition should apply regardless of whether the entity acting on the consumer's behalf has a fiduciary duty. This definition would be in keeping with existing law, which defines the term "financial product or service" without reference to fiduciary duties. Additionally, this definition allows a wide variety of entities to qualify as representatives, which will help improve competition across a wide variety of industries and expand consumer choice and welfare. However, authorized representatives must take commensurate responsibility and assume liability for their handling of the consumer data they request, as discussed below.

Question 8: To maximize competition, the broad definition of "representative" should be paired with a tailored definition of "covered person." In particular, CFPB should reconsider its

[1] CCIA is an international nonprofit membership organization representing companies in the computer, Internet, information technology, and telecommunications industries. Together, CCIA's members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue. CCIA promotes open markets, open systems, open networks, and full, fair, and open competition in the computer, telecommunications, and Internet industries. A complete list of CCIA members is available at http://www.ccianet.org/members.

prior classification of digital wallets as "covered persons" under this rule. Instead, this rule should define "covered persons" only as accounts offering debit, credit, and/or investment services, and exclude digital wallets that merely serve as pass-through intermediaries and do not store underlying account information, approve or deny transactions, or otherwise function as traditional financial entities. This would better align the U.S. system with how other systems, such as the UK, approach open banking.[2] Moreover, including digital wallets in the definition of "covered person" imposes duplicative compliance obligations while yielding little meaningful data, and unnecessarily risks compromising data. These risks decrease the consumer and developer trust that is necessary for open banking to succeed.

II. Defraying of Costs

Question 10: The CFBP can take further measures to minimize interference with the data access right envisioned by Congress by requiring covered persons to share information about how consumers can initiate payments across all available payment networks. Providing such information is important for facilitating pay-by-bank transfers and other modern payment options. Such a rule would help ensure seamless transactions between covered persons and authorized representatives, and would expand the number of payment options available to consumers.

Question 13: The risk of unauthorized representation can be mitigated by assigning liability to the authorized representative for any harm resulting from inadequate privacy and cybersecurity practices while the consumer data is in the authorized representative's possession. To provide greater certainty, the rule should advance an expanded liability framework under which each participant in the data-sharing chain bears responsibility for breaches or misuse of data that occurs during the period it controls the data.

III. Addressing Cybersecurity Concerns

[2] *See, e.g.*, Retail Banking Market Investigation Order 2017, UK Competition & Mkts. Auth., *available at* https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf.

Question 18: Without adequate safeguards, the rule risks undermining security. Generally, larger firms will be subject to more stringent cybersecurity requirements than smaller ones.[3] Consumers should not have their data security jeopardized when data is transferred to a company that is held to lower cybersecurity standards. Additionally, the rule could increase the risk of fraud and data breaches, requiring that covered persons share sensitive consumer data with third parties whose data practices they have not vetted.

To avoid these problems, this rule should specify that while the authorized representative possesses consumer data requested pursuant to this rule, the authorized representative (rather than the covered person sharing the data) is responsible for safeguarding it, as noted above. It should further specify that covered persons are not liable for harms to consumers resulting from their authorized representatives' inadequate cybersecurity precautions. This policy would incentivize authorized representatives to adopt stronger cybersecurity protocols and would allocate liability risks to those companies that have implemented fewer such safeguards. This incentive structure would lead to an overall increase in consumer data protection.

Question 27: Overly prescriptive standards should be avoided. A longstanding principle in crafting cybersecurity standards is that different entities require different levels of cybersecurity protection based on their size and the type of data they process.[4] The existing standards under GLBA should provide sufficient protection. However, as noted above, assigning responsibility for safeguarding the requested data to the authorized representative (rather than the covered person sharing the data) during the time the authorized representative possesses the data would incentivize representatives to increase their cybersecurity standards to the greatest extent possible.

---

[3] *See, e.g.*, *Exchange Act Reporting*, SEC (Sep. 22, 2025), https://www.sec.gov/resources-small-businesses/going-public/exchange-act-reporting-registration (outlining differing reporting requirements for companies based on size); California Consumer Privacy Act, Cal. Civ. Code § 1798.140(d)(1) (West 2025) (listing size and revenue criteria for determining which businesses must comply with the law). Both sets of rules confer additional cybersecurity requirements on companies meeting the listed thresholds.

[4] *See, e.g.*, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29 §§ 3.1-3.2 (February 24, 2024), *available at* https://www.nist.gov/cyberframework (outlining the concepts of CSF profiles and tiers to determine cybersecurity standards for different types and sizes of businesses).

IV. Addressing Privacy Concerns

Question 30: The privacy concerns under this rule parallel the cybersecurity concerns. Without the liability standard described above, consumers' sensitive information risks being exposed if transferred to an entity that does not adhere to stringent privacy standards. However, the above liability standard would help address this problem by encouraging authorized representatives to maintain high privacy standards. Additionally, it would discourage authorized representatives from requesting data they do not need, thus minimizing the number of locations in which consumer data is stored.

V. Setting Compliance Dates

Question 36: Building and maintaining secure developer interfaces to securely share data with many third parties is a large and complex task. This infrastructure will require significant financial and personnel commitments from covered entities. Significant lead time is therefore necessary, particularly as the specific requirements for such interfaces have not yet been announced. A 24-month window starting on the date when technical requirements are first made available should be sufficient for covered entities to ensure compliance.

Respectfully submitted,

Jesse Lieberfeld
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
jlieberfeld@ccianet.org

10/20/2025