epic.org

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

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

March 17, 2025

U.S. House Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair Hill, Ranking Member Waters, and Members of the Committee,

The Electronic Privacy Information Center (EPIC) provides this statement for the record for the hearing entitled "Updating America's Financial Privacy Framework for the 21st Century." EPIC is an independent nonprofit research organization established in 1994 to secure the right to privacy in the digital age for all people. We have appreciated the opportunity to provide input to the Committee on similar topics in the past, including through testimony at the December 2024 hearing entitled "Innovation Revolution: How Technology is Shaping the Future of Finance" and through our recent letter and comment in response to the Committee's request for feedback on current federal consumer financial data privacy law.[1]

EPIC promotes legal and technological standards that strengthen privacy protections for individuals in the digital economy. We support innovations that make financial services more secure, resilient, and accessible for consumers. However, we have also seen a broad and troubling trend toward commodifying and monetizing personal data, including sensitive financial data, in ways that enrich data brokers and other businesses at the expense of consumers. In order to promote innovations in this sector that will empower consumers rather than exploiting them, we need privacy and security protections that are fit for the 21st Century.

1. **Maintaining the privacy and security of financial information is paramount for consumers and national security.**

Financial information is particularly sensitive. If financial information is breached, fraudsters and scammers may gain access to the information, which could lead to significant financial loss for the victims of the breach. For example, fraudsters may use personal financial data to target victims for scams. Financial data can also be used to legitimize fraud schemes.[2] If a fraudster contacts an individual claiming to be a representative from the individual's bank, the

[1] *EPIC, NCLC, and 45 Other Organizations Call on Congress to Strengthen Financial Privacy,* EPIC (Sept. 2, 2025), https://epic.org/epic-nclc-and-45-other-organizations-call-on-congress-to-strengthen-financial-privacy/.
[2] *Phishing Scams*, American Bankers Association, https://www.aba.com/advocacy/communityprograms/consumer-resources/protect-your-money/phishing (last visited Aug. 12, 2025).

person is more likely to fall for the scheme if the fraudster provides accurate information related to the individual's bank account.[3] A report by the Federal Trade Commission estimated that consumers lost over $195.9 billion to fraud in 2024 alone.[4]

Protecting the security of financial information is also critical for national security. If data held by financial institutions is exposed in a breach, criminals and foreign adversaries could 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 they hold may include financial information exposed in such incidents. Data brokers compile and sell detailed profiles about individuals, often without implementing adequate security controls to prevent the data from ending up in the wrong hands. Duke University researchers found that data brokers sell profiles containing sensitive information about active-duty military members, veterans, and their families for as little as $0.12 per record.[5] Further, a report by the Irish Council for Civil Liberties revealed 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, used by data brokers to target online ads.[6] Bad actors can use sensitive financial information purchased from data brokers to blackmail or facilitate phishing tactics to obtain state secrets from military and government personnel.[7] The Committee must work to limit the sale of financial data and ensure that financial institutions maintain strong privacy and data security standards so that financial information is not used to threaten national security.

Financial institutions must follow strong, robust privacy and data security standards, both to protect individuals from financial harm and prevent the misuse of financial information that could threaten our national security. We urge the Committee to keep these serious risks in mind,

---

[3] *Id*.
[4] *Protecting Older Consumers 2024-2025*, Federal Trade Commission (Dec. 1, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.
[5] 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-ofdataon-us-military-personnel/.
[6] 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-audiencesegments-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/Americashidden-securitycrisis.pdf.
[7] 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-remarksofcfpb-director-rohit-chopra-at-the-white-house-on-data-protection-and-nationalsecurity/.

especially given the ways in which modern technology can be used to supercharge the dissemination of personal data.

2. The financial services of the future should not be built on the privacy models of the past, and clear rules limiting data collection and use are needed.

The rapid growth of financial technology over the last decade has led to major changes in how people transact, invest, and store value in a digital ecosystem. One aspect of this change is an exponential growth in the amount of data collected about individuals, along with a fundamental shift in how that data is used and the impact those uses have on consumers. As technologies and business practices in the financial services industry have shifted, the privacy protections and standards have not kept pace. Our current financial privacy regime is rooted in outmoded understandings of both the boundaries of the field and the scope of protections necessary to preserve privacy. We need a new approach as we look ahead toward future developments in financial technology over the next two decades.

Specifically, we urge the Committee not to expand or extend the GLBA's notice-and-choice regime because this approach is outdated and fails to provide sufficient privacy protections for consumers.[8] The GLBA requires financial institutions to provide customers with privacy notices and give consumers a (limited) opportunity to opt out of some (limited) types of data sharing. Notice-and-choice style laws like the GLBA place the impossible burden on consumers to protect their own privacy. The privacy policies provided by financial institutions are vague and expansive; these policies are written to protect companies from liability rather than to ensure that consumers are fully empowered to make privacy choices. We have all received notices from financial institutions in the mail containing pamphlets with disclosures about all the ways in which a bank or credit card company will disclose our data to other entities. In reality, very few customers read these privacy notices. In any case, most of the information contained within the privacy notices is drawn from the Model Privacy Form,[9] so terms are repetitive and not open for negotiation even if consumers do read them. Further, the GLBA's opt-out provisions include a number of exemptions, so even if consumers do read the privacy notices and choose to opt out of data sharing, their choice to opt out will not always be honored.

Regardless of its substantive provisions, GLBA should remain a federal floor for financial data privacy protection, rather than preempting stronger state laws. The GLBA was passed over 25 years ago and has not been updated to address the increasing technology-driven

[8] EPIC Statement Re: Data Privacy Act of 2023, EPIC (Feb. 27, 2023), https://epic.org/documents/epicstatement-re-data-privacy-act-of-2023/.
[9] Model Privacy Form under the Gramm-Leach-Bliley Act, https://www.sec.gov/files/rules/final/2009/34-61003_modelprivacyform.pdf (last visited Mar. 13, 2026).

harms since, and, even if Congress updates GLBA in 2026, technology will continue to change. States must be able to adapt to this changing technology and provide strong privacy protections for their constituents. Congress should not prevent states from establishing stronger and more effective regulatory standards to protect financial privacy.

Many states have already begun to adopt comprehensive privacy regimes. Making the GLBA a preemptive standard without amending the GLBA to include significantly stronger privacy protections would contract the scope of privacy protections by annulling already passed laws in many states. Any federal privacy law must include data minimization protections that limit the collection and use of personal data to what is necessary to provide the product or service the consumer requested.[10] Data minimization protections ensure that companies' data practices align with consumers' expectations. The American Data Privacy and Protection Act of 2022 (ADPPA)[11] and the American Privacy Rights Act of 2024 (APRA),[12] which were both developed through bipartisan and bicameral processes, included strong data minimization standards, and states have begun to enact these standards into law.[13] Given the scope of modern day data collection and use, the Committee must work to establish meaningful limits on companies' collection, retention, sharing, and sale of personal data. In contrast with the notice-and-choice framework, these protections would better align companies' data practices with consumer expectations.

3. Regulators should be empowered to monitor, investigate, and enforce violations of financial protection laws.

After the rapid expansion of consumer credit and the emergence of the credit reporting bureaus in the 1970s, fairness became a central focus of policymaking in the financial sector. The Fair Credit Reporting Act (FCRA) was the first federal consumer privacy law in the U.S., and it was enacted alongside the Equal Credit Opportunity Act and the Fair Credit Billing Act to establish significant guardrails for the evolving financial services sector. These laws addressed the problems of increasing complexity, velocity, and automation in the field by establishing enforceable individual rights for consumers to protect against increased fraud, discrimination,

[10] *EPIC Feedback to House Energy & Commerce Majority Privacy Working Group*, EPIC (Apr. 2025), https://epic.org/documents/epic-feedback-to-house-energy-commerce-majority-privacy-working-group/ (citing Caitriona Fitzgerald & Kara Williams, *Data Minimization Is the Key to a Meaningful Privacy Law*, EPIC (May 2024), https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/.)
[11] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. Title I (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.
[12] American Privacy Rights Act (APRA), H.R. 8818, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/8818/text.
[13] *See e.g.* Maryland Online Data Privacy Act, Md. Code Ann., Com. Law § 14-4707.

and inaccurate reports that these new technologies and business practices would cause. And without them, consumers would have been much worse off.

Congress continued to meet the moment to protect consumers in 2010 when it passed the Dodd-Frank Act, which created the Consumer Financial Protection Bureau (CFPB). This authorizing legislation imposes important mandatory responsibilities on the CFPB, including responding to consumer complaints in a timely manner and conducting routine supervision of both depository institutions (banks) and non-depository institutions (nonbank financial institutions, such as private lenders). Since its creation, the CFPB has obtained over $21 billion in reimbursements and forgiven debt for consumers.[14]

Recently, the CFPB has been under attack, with its staffing and funding severely limited. The CFPB was established to play a critical role in the financial marketplace: supervising financial institutions, establishing regulations to implement consumer financial protection laws, and bringing enforcement actions to remedy violations of consumer financial protection laws. Consumers and financial institutions alike are worse off after the CFPB's expertise, capability, and oversight have been exponentially diminished. We urge the Committee to work to reinstate the CFPB's staffing and funding so that the Bureau can continue its essential work to protect consumers from harm in the financial marketplace.

We also urge the Committee to work with the CFPB to maintain the previously finalized rules issued by the CFPB to implement Section 1033 of the Dodd-Frank Act.[15] These rules, which are currently being reconsidered by the CFPB,[16] included strong data minimization requirements, prohibitions against selling/sharing information or use for targeted marketing without consent (i.e., a prohibition against secondary use), accuracy and error resolution provisions, a right to revoke access and delete data, and time limits on data access. We hope that the Bureau retains these best-in-class privacy protections, and we urge the Committee to express support for the strong financial privacy protections included in the Section 1033 rules finalized by the CFPB in October 2024.

---

[14] *The CFPB*, Consumer Financial Protection Bureau (2026), https://www.consumerfinance.gov/about-us/the-bureau/.

[15] 12 C.F.R. Part 1033; *Final Rule – Required Rulemaking on Personal Financial Data Rights*, Consumer Financial Protection Bureau (Oct. 2024), https://files.consumerfinance.gov/f/documents/cfpb_personal-financial-data-rights-final-rule_2024-10.pdf.

[16] Advance Notice of Proposed Rulemaking - Personal Financial Data Rights Reconsideration, Consumer Financial Protection Bureau (Aug. 2025), https://www.federalregister.gov/documents/2025/08/22/2025-16139/personal-financial-data-rights-reconsideration.

4. EPIC Opposes *H.R.____, a bill to make improvements to title V of the Gramm-Leach-Bliley Act, and for other purposes*

While EPIC appreciates your attention to the need for improved privacy protections in the financial services sector, we have grave concerns about the discussion draft noticed for today's hearing. We urge the Committee not to advance this bill because it would extend outdated GLBA instead of providing necessary, strong, and effective privacy and data security protections for consumers in the financial marketplace.

Sec. 102 Data Minimization

The data minimization standard currently included in the bill provides weak privacy protections for consumers. Currently, the language permits financial institutions to collect, use, retain, or disclose information for any "legitimate business, legal, or regulatory purpose." This standard is too broad and would provide essentially the same level of privacy protection as a notice-and-choice framework because it would allow businesses to collect and use data for any purpose an institution deems legitimate, even if those purposes are contrary to consumers' expectations. For example, this provision may allow financial institutions to sell customers' purchase records to data brokers for advertisement targeting. We recommend strengthening the language to limit the collection and use of personal data to what is reasonably necessary to provide the product or service the consumer requested.[17]

Sec. 507. Relation to State Laws

We recommend removing this provision because it would amend the GLBA to preempt stronger state privacy legislation, thereby diminishing consumer financial privacy and increasing the risk of data breaches, fraud, scams, and other financial harm.[18] As discussed in more detail above in response to Question 2, the GLBA relies on an outdated, ineffective notice-and-choice framework that does not provide sufficient privacy and data security protections for consumers. Preempting state laws relating to consumer privacy and data security for financial institutions

---

[17] *Data Minimization*, EPIC (2026), https://epic.org/issues/consumer-privacy/data-minimization/; *EPIC Feedback to House Energy & Commerce Majority Privacy Working Group*, EPIC (Apr. 2025) https://epic.org/documents/epic-feedback-to-house-energy-commerce-majority-privacy-working-group/; Caitriona Fitzgerald & Kara Williams, *Data Minimization Is the Key to a Meaningful Privacy Law*, EPIC (May 2024), https://epic.org/data-minimization-is-the-key-to-a-meaningful-privacy-law/.

[18] In re: Request for Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals, EPIC and NCLC (Aug, 2025), https://epic.org/wp-content/uploads/2025/09/EPIC-NCLC-HFSC-financial-privacy-comment.pdf; Letter to House Financial Services Committee Re: Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals, EPIC, NCLC, et. al. (Aug. 2025), https://epic.org/wp-content/uploads/2025/09/Letter-to-House-FSC-Modernize-Financial-Data-Privacy-without-Nullifying-State-Protections-with-sign-ons.pdf.

subject to GLBA would have serious consequences, and state legislatures should be permitted to provide stronger protections for their constituents if changes in technology necessitate it. Further, this provision essentially establishes an entity-level exemption from state laws for GLBA-covered institutions, leaving the data that financial entities collect on their websites and apps unregulated. Establishing an entity-level GLBA exemption goes against the trend in states, which have recently started narrowing exemptions to only GLBA-covered data, not GLBA-covered entities as a whole.

* * *

There is no doubt that we are witnessing rapid changes in financial technology. This Committee has an opportunity to support legislation that protects the privacy and data security of financial information, which in turn will build trust within the financial marketplace. Congress also has an opportunity to support and empower regulators like the CFPB to shut down unfair practices before they can take root and spread financial hardship.

We ask that this letter be entered in the record, and we look forward to continuing to work with the Committee to advance privacy, security, and consumer rights in the financial marketplace.

Sincerely,

/s/ Caroline Kraczon
Counsel
Electronic Privacy Information Center

/s/ Alan Butler
Executive Director
Electronic Privacy Information Center

/s/ Caitriona Fitzgerald
Deputy Director & Policy Director
Electronic Privacy Information Center