August 28, 2025

The Honorable French Hill
Chair, House Committee on Financial Services
The Honorable Andy Barr
Chair, Subcommittee on Financial Institutions
United States House of Representatives, Financial Services Committee
2129 Rayburn House Office Building
Washington, DC 20515

In re: Request for Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals

Dear Chairman Hill, Chairman Barr, and members of the United States House Committee on Financial Services,

The Electronic Privacy Information Center (EPIC)[1] and the National Consumer Law Center (NCLC)[2] appreciate the opportunity to provide feedback on federal consumer financial privacy law to the House Committee on Financial Services. As the Committee considers potential legislative proposals to keep pace with changes in the financial services industry, it must ensure that financial privacy law adequately protects the privacy, accuracy, and security of Americans' personal financial data. The Gramm-Leach-Bliley Act (GLBA) fails to effectively protect the privacy of consumers'

[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. *See About Us*, EPIC, https://epic.org/about/ (2024). EPIC has long advocated for privacy rights and robust safeguards to protect consumers, including in the financial sector. *See, e.g. 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-to-protect-consumer-financial-privacy/; 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-epic-and-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/epic-executive-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/epic-submits-comments-to-strengthen-cfpb-proposals-for-financial-data-rights-rulemaking/.

[2] The National Consumer Law Center (www.nclc.org) is a nonprofit organization specializing in consumer issues on behalf of low-income people. We work with thousands of legal services, government and private attorneys, as well as community groups and organizations, from all states who represent low-income and elderly individuals on consumer issues. As a result of our daily contact with these advocates, we have seen many examples of exploitation of consumer data, violations of consumer privacy, and the damage wrought by abuses from credit and consumer reporting agencies from every part of the nation. It is from this vantage point that we supply these comments. Fair Credit Reporting (10th ed. 2022) is one of the eighteen practice treatises that NCLC publishes and annually supplements. NCLC submits these comments on behalf of its low-income clients.

financial information. Congress must strengthen privacy protections for Americans' financial data, preferably through a federal comprehensive privacy law.

Maintaining the privacy, accuracy, and security of personal financial information is critical because 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.[3] 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.[4] A report by the Federal Trade Commission estimated that consumers lost over $158 billion to fraud in 2023 alone.[5] The Committee must ensure that financial institutions follow strong privacy and data security standards to help 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 ensure that the data does not end up in the wrong hands. Duke University researchers found that data brokers sell profiles containing sensitive information of active-duty military members, veterans, and their

[3] *Phishing Scams*, American Bankers Association, https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/phishing (last visited Aug. 12, 2025).
[4] *Id*.
[5] *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.

families for as little as $0.12 per record.[6] 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 brokers use to target online advertisements.[7] 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.[8] The Committee must limit the sale of financial data and ensure that financial institutions follow sufficient privacy and data security standards so that financial information is not used to threaten national security.

Ensuring the accuracy of financial information is critical given the many important purposes for which that data can be used. Credit reports and specialty consumer reports can determine a consumer's access to a bank account, affordable credit, rental housing, insurance and even employment.[9] Deposit account information is used for a multitude of purposes, such as tax cashflow underwriting, tax preparation, payment platforms (e.g., Venmo), and personal financial management.[10] Errors in credit reports or bank account information can cost a consumer thousands of dollars in higher mortgages or insurance rates, shut them out of the banking system, deny them a

---

[6] 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/.

[7] 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.

[8] *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/.

[9] See Chi Chi Wu and Ariel Nelson, *Mission Creep: A Primer on Use of Credit Reports & Scores for Non-Credit Purposes*, NCLC (Aug. 2022), https://www.nclc.org/resources/mission-creep-a-primer-on-use-of-credit-reports-scores-for-non-credit-purposes/

[10] NCLC, Comments to CFPB on Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB–2023–0052 (Dec. 28, 2023), https://www.nclc.org/wp-content/uploads/2024/01/NCLC-comments-to-Section-1033-NPRM.pdf.

much-needed job, or even prevent them from getting the basic human need of shelter. To combat fraud, financial institutions collect extensive information about how users behave and transact, then build sophisticated tools and systems to identify fraud patterns. If the proper guardrails to ensure the accuracy of this information are not put into place, innocent consumers will be harmed.

Financial institutions must follow strong, robust privacy and data security standards, both to protect individuals from financial ruin and to help ensure that financial information cannot be used to undermine our national security. The Committee should keep these serious risks in mind when evaluating whether current financial protection law provides adequate protection, especially given the ways in which technology can be used to supercharge the dissemination of personal data. We appreciate that the Committee is considering how it may strengthen financial privacy laws, and we would welcome the opportunity to continue to engage with the committee on this topic.

Response to Question 1: Should we amend the Gramm-Leach-Bliley Act (GLBA) or consider a broader approach?

The GLBA utilizes a notice-and-choice approach to regulate the collection of consumers' financial information—this regime is outdated and fails to provide sufficient privacy protections for consumers.[11] The GLBA requires financial institutions to provide customers with privacy notices and give consumers an opportunity to opt out of some (limited) types of data sharing. 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.[12] 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. Further, the GLBA's opt-out provisions include a number of exemptions, so even if consumers do read the

[11] *EPIC Statement Re: Data Privacy Act of 2023*, EPIC (Feb. 27, 2023), https://epic.org/documents/epic-statement-re-data-privacy-act-of-2023/.
[12] *Id*.

privacy notices and choose to opt out of data sharing, their choice to opt out will not always be honored and consumers are not empowered to make meaningful choices to protect their privacy. The Committee must not expand or extend the GLBA's notice-and-choice regime because it does not provide meaningful privacy protections to consumers.

The Committee has an opportunity to propose legislation that meaningfully protects the privacy of consumers' financial information. Notice-and-choice style laws like the GLBA place the impossible burden on consumers to protect their own privacy. Instead of extending or expanding on the GLBA, Congress should pass comprehensive privacy legislation that limits the abuse of personal data.

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.[13] Data minimization protections ensure that companies' data practices align with consumers' expectations. The American Data Privacy and Protection Act of 2022 (ADPPA)[14] and the American Privacy Rights Act of 2024 (APRA),[15] which were both developed through bipartisan and bicameral processes, included data minimization standards. Congress should continue to develop strong, comprehensive federal privacy legislation that builds on ADPPA and APRA. Data minimization is discussed in further detail in response to Question 13.

In addition to strong data minimization rules, a federal comprehensive privacy law should also include basic privacy rights that many states have incorporated into their own privacy laws. These rights include the right to access, correct, and delete personal information, the right to opt out of the processing of the consumer's personal data for targeted advertising or profiling, the right to

[13] *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/.)
[14] 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.
[15] American Privacy Rights Act (APRA), H.R. 8818, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/8818/text.

opt out of the sale of personal data, and the right to obtain a list of third parties to whom a controller has disclosed the consumer's personal data.[16] Most states that have passed general privacy laws have also required that companies obtain a consumer's opt-in consent before processing sensitive data, which in some states includes financial data. As discussed below, an affirmative opt in should, at minimum, be required for the sharing of financial information or its use for targeted marketing. Congress must also ensure that consumers are able to exercise their privacy rights by including a provision that allows consumers to use an authorized agent to exercise privacy rights on their behalf and require companies to recognize a universal opt-out mechanism.[17] As discussed further in response to Question 12, a federal privacy law should also include a private right of action.

Any federal privacy law must also include protections against data-driven discrimination. Covered entities must be prohibited from using personal data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.[18] Further, consumers must not face the threat of discrimination based on whether they choose to exercise their privacy rights. Controllers should be prohibited from charging a different price or offering a different level or quality of product or service because a consumer exercised their privacy rights.

A federal privacy law should also include heightened protections for sensitive personal information. As explained above, financial information is especially sensitive. Consumers go to great lengths to protect the privacy of their personal financial data, and there are serious financial and national security risks if financial information is breached. Legislators in California,[19] New Jersey,[20] and Connecticut[21] have included financial information within the definition of "sensitive personal information," providing heightened privacy protections for this category of data. The

[16] *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/.
[17] *Id.*
[18] *Id.*
19 Cal. Civ. Code § 1798.140(ae)(1)(B).
20 N.J. Stat. § 56:8-166.4.
21 Conn. Gen. Stat. § 42-515(39)(H).

Committee should work with the rest of Congress to ensure that a comprehensive federal privacy bill includes heightened protections for financial information. These heightened protections should include both a prohibition on the sale or sharing of sensitive personal information, a prohibition against its use for targeted marketing, and a requirement that any collection, processing, or transferring of sensitive personal information be limited to circumstances where such use is strictly necessary. Congress also should require users of sensitive personal information to notify consumers when this information is used against them, similar to the adverse action notice requirement of the Fair Credit Reporting Act (FCRA).[22]

The use of aggressive fraud detection tools by banks to shut their own customers from accounts illustrates why an adverse action notice requirement is critical.[23] The number of accountholders who complained about checking and savings account closures to the CFPB more than doubled from 2017 to January 2025.[24] There have also been stories featured by reporters detailing the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived access to their funds, are not provided with any information about the reason for the institution's actions, and are not provided an opportunity to address any perceived risk.[25] The impact of sudden account closures in response to potential fraud on innocent consumers

[22] 15 U.S.C. § 1681m(a).

[23] For example, in 2022, the CFPB ordered Wells Fargo to pay $160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it "believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system." *See In the Matter of Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (Dec. 20, 2022) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

[24] CFPB Consumer Complaint Database trends data for complaints received due to checking or savings account closure available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&dateRange=All&date_received_max=2024-01-27&date_received_min=2011-12-01&has_narrative=true&issue=Closing%20an%20account%E2%80%A2Company%20closed%20your%20account&lens=Product&product=Checking%20or%20savings%20account&searchField=all&subLens=sub_product&tab=Trends.

[25] Barnard, Tara Siegel and Lieber, Ron, "*Banks Are Closing Customer Accounts, With Little Explanation*," New York Times (Apr. 8, 2023) available at https://www.nytimes.com/2023/04/08/your-money/bank-

cannot be overstated. Often, the most vulnerable people have been denied access to their money, rendering them unable to eat or pay rent. Such impacts show why it is also imperative to have error resolution procedures in place to enable people to dispute account freezes and closures and get their money back as soon as possible.

If there are exceptions allowing for sharing of information for fraud prevention in an expanded federal privacy regime, innocent consumers must be protected with requirements that (1) the shared information must be accurate and not misleading; and (2) if the shared information leads to an adverse action, such as an account freeze or closure, the consumer must be given a notice and; (3) the consumer must be given the opportunity to dispute the inaccuracy of any shared information and the financial institution must be required to conduct an investigation of the consumer's dispute.

Response to Question 2: Should we consider a preemptive federal GLBA standard or maintain the current GLBA federal floor approach?

The 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 respond to increasing technology-driven harms since. States must be able to adapt to changing technology and provide strong privacy protections for their constituents. Many states have already begun to adopt comprehensive privacy regimes, which is explained further in response to Question 8.

As discussed in response to Question 1, the GLBA does not effectively protect consumer financial privacy. Making the GLBA a preemptive standard without passing a strong federal

---

account-suspicious-activity.html?unlocked_article_code=1.QU0.szRm.kfoZRQdD7-O6&smid=url-share; Kessler, Carson, "*A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money*," ProPublica (July 6, 2021), available at https://www.propublica.org/article/chime; McGreevy, Patrick, "*Bank of America must provide more proof of fraud before freezing EDD accounts, court orders,*" Los Angeles Times (Jun. 1, 2021), available at https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california; KCAL News, "*Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud*," (Oct. 29, 2020), available at https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/.

comprehensive privacy bill or amending the GLBA to include the strong privacy protections recommended in response to Question 1 would contract the scope of privacy protections by annulling already passed laws in many states. Congress should not prevent states from establishing stronger and more effective regulatory standards to protect financial privacy.

Even if the GBLA were strengthened, it would be significantly harmful to consumers to allow the Act to preempt state laws because its scope of coverage is so broad. The definition of "financial institution" in the GLBA is not limited to banks, credit unions, or other depository institutions. Instead, it covers a gamut of non-depository businesses, such as consumer reporting agencies (CRAs) and debt collectors, [26] as well as auto dealers, travel agents, check cashers, tax preparers, and many other businesses.[27]

Adopting a provision that the GLBA preempts stronger state laws would prevent states from regulating the privacy and data practices of all of these businesses. Moreover, it could potentially preempt a number of existing state privacy and consumer protection laws, including laws that should serve as a model for federal legislation such as the California and Maryland laws discussed in response to Question 8. Because of the wide scope of GLBA's coverage of "financial institutions," amending the Act to be preemptive could possibly affect sector-specific laws and result in:

- Annulling state laws in over half of the states (27 states plus Puerto Rico) that govern credit reports, and in some cases, other types of consumer reports.[28]

[26] GLBA defines "financial institution" as businesses engaged in activities as described in section 1843 of the Bank Holding Company Act of 1956 (12 U.S.C. 1843). 15 U.S.C. § 6809; 12 C.F.R. § 1016.3(l)(1). The regulation implementing that Act refers specifically to both collection agency activities in (b)(2)(iv) and credit bureau services in (b)(2)(v). 12 C.F.R. § 225.28. *See also* Trans Union, L.L.C. v. Fed. Trade Comm'n, 295 F.3d 42, 48, 49 (D.C. Cir. 2002) (FTC permissibly determined that a CRA is a "financial institution" subject to the rulemaking authority of the FTC under the Act)). *See generally*, National Consumer Law Center, Fair Credit Reporting (10th ed. 2022) § 18.4.1.3, updated at www.nclc.org/library.

[27] 12 C.F.R. § 1016.3(l)(3). *See generally*, National Consumer Law Center, Fair Credit Reporting (10th ed. 2022) § 18.4.1.3, updated at www.nclc.org/library.

[28] These states include AZ, AR, CA, CO, CT, GA, KS, LA, ME, MD, MA, MD, MT, NE, NV, NH, NJ, NM, NY, OH, OK, PR, RI, SC, TX, UT, VT, WA. For citations and summaries, see Appendix H of National Consumer Law Center, Fair Credit Reporting (10th ed. 2022), updated at www.nclc.org/library.

- Preventing states and localities from regulating tenant screening companies, which are considered CRAs, in order to protect tenants and address the current crisis in rental housing.[29]
- Nullify all 15 of the recently enacted state laws prohibiting medical debt on credit reports, which advance the common-sense idea that people should not be denied loans, insurance, or jobs just because they got sick.[30]

Preempting state laws would also stop necessary advances in privacy protections for changing times and practices. For example, it would have prevented California from adopting its first-in-the-nation Financial Information Privacy Act,[31] which has an opt in regime not opt out, for sharing data with nonaffiliated third parties. In the federalist system adopted by our Founders, states serve as the laboratories of experimentation. We have seen at least 19 states enact general consumer privacy laws. Congress recently recognized the importance of state law regulation of new technologies when it removed from the just-passed reconciliation bill a provision that would have preempted state laws that would protect consumers with regards to artificial intelligence.[32]

We have also seen what happens when financial institutions are carved out of state privacy protections. A number of states have adopted exemptions for GLBA-regulated entities from their general consumer privacy laws.[33] This has resulted in the bizarre irony that big banks are less regulated in their privacy practices than ordinary retailers, despite the former having far more sensitive and valuable information about their customers than the latter. Further, state Attorneys

[29] For example, Colorado prohibits CRAs from including sealed or expunged criminal records in consumer reports. Colo. Rev. Stat. § 5-18-105.
[30] CA, CO, CT, DE, IL, MD, ME, MN, NJ, NY, OR, RI, VT, VA, WA. See Chi Chi Wu, National Consumer Law Center, The Latest on Keeping Medical Debt Out of Credit Reports, July 30, 2025, https://library.nclc.org/article/latest-keeping-medical-debt-out-credit-reports
[31] Cal. Fin. Code §§ 4050 to 4060.
[32] David Morgan and David Shepardson, *US Senate strikes AI regulation ban from Trump megabill*, Reuters, July 1, 2025, https://www.reuters.com/legal/government/us-senate-strikes-ai-regulation-ban-trump-megabill-2025-07-01/
[33] *See* Caroline Kraczon and Justin Sherman, Electronic Privacy Information Center, *Unbridled and Underregulated: Removing FCRA and GLBA Exemptions from Privacy Laws to Hold Data Brokers Accountable*, July 2025, https://epic.org/documents/unbridled-and-underregulated-removing-fcra-and-glba-exemptions-from-privacy-laws-to-hold-data-brokers-accountable/

General have already noted that GLBA exemptions hampers their ability to enforce state consumer privacy laws.[34]

Response to Question 4: How should GLBA relate to other federal consumer data privacy laws, both a potential general data privacy law and current sector-specific laws? Should GLBA "financial institutions" be subject to entity-level or data-level exemptions from these laws?

Federal consumer privacy laws should not include any exemptions for financial institutions covered by the GLBA. As discussed in response to Question 1, the GLBA currently fails to provide adequate consumer protections for financial privacy and data security. The data held by financial institutions is highly sensitive and ripe for abuse if it falls into the wrong hands. Congress must strengthen privacy and data security protections for consumers by passing a strong general data privacy law including the provisions recommended in response to Question 1, and GLBA-covered financial institutions and data should not be exempt from those protections.

GLBA-covered data and entities should also not be exempt from other sector-specific laws. For example, credit reporting and other consumer agencies are often within the scope of both the GLBA and the FCRA. The FCRA provides stronger consumer protections than the GLBA, including:

- stronger limitations on third-party access to data, by requiring users have a permissible purpose to obtain a consumer report,[35]
- requirements for companies to follow reasonable procedures for maximum possible accuracy, [36]
- the right to correct inaccurate data, [37]
- the right to access data contained in one's credit file, [38]

[34] *See* UPDATED ENFORCEMENT REPORT PURSUANT TO CONNECTICUT DATA PRIVACY ACT, CONN. GEN. STAT. § 42-515, ET SEQ., State of Connecticut Office of the Attorney General (Apr. 17, 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf.
[35] 15 U.S.C. § 1681b.
[36] 15 U.S.C. § 1681e(b).
[37] 15 U.S.C. §§ 1681i(a), 1681s-2.
[38] 15 U.S.C. § 1681g.

- several identity theft protections, including the right to prevent access to information in certain circumstances (security freeze), [39] and
- in general, stronger notice and transparency provisions.[40]

If Congress amended the FCRA to include an exemption for GLBA-covered data or entities, it would literally gut the former, since consumer reporting agencies are considered "financial institutions" under GLBA – there would be nothing left for the FCRA to regulate. The GLBA does not provide anywhere near the privacy, procedural and substantive protections of the FCRA.

Similarly, Section 1033 of the Dodd-Frank Act provides consumers with the right to access information in their financial accounts,[41] which is not a right that the GLBA provides, and its implementing rule has a robust privacy and consumer protection regime as discussed in the response to Question 8. The HIPAA Privacy Rule provides for strong limitations on third-party access to health information.[42] The Family Educational Rights and Privacy Act provides a privacy and consumer protection regime for educational data. [43] Congress must not weaken any of these protections by including exemptions for GLBA-covered financial institutions or covered data in these and other federal privacy and consumer protection laws.

Response to Question 8: Are there states that have developed effective privacy frameworks? Which specific elements from these state-level frameworks could potentially be adapted for federal implementation?

As of August 2025, nineteen states have passed general privacy laws. Unfortunately, the majority of state privacy laws rely on the notice-and-choice framework. As discussed in response to Question 1, notice-and-choice places the burden of privacy protection on consumers and fails to

[39] 15 U.S.C. §§ 1681c-1, 1681c-2.
[40] *See* Caroline Kraczon and Justin Sherman, *Unbridled and Underregulated: Removing FCRA and GLBA Exemptions from Privacy Laws to Hold Data Brokers Accountable*, Electronic Privacy Information Center (July 2025), https://epic.org/documents/unbridled-and-underregulated-removing-fcra-and-glba-exemptions-from-privacy-laws-to-hold-data-brokers-accountable/.
[41] 12 U.S.C. § 5533.
[42] 45 C.F.R. Parts 160 and 164.
[43] 20 U.S.C. 1232g.

provide meaningful privacy protections. In contrast, California and Maryland have both passed stronger privacy laws that utilize a data minimization framework.[44] The Maryland Online Data Privacy Act (MODPA) takes inspiration from the data minimization standards included in the ADPPA and the APRA. The law, which goes into effect on October 1, 2025, requires that companies limit their collection of personal data to what is *reasonably necessary to provide the product or service the consumer requested*. The MODPA's data minimization framework effectively aligns companies' data collection practices with what consumers expect. Federal privacy legislation must include strong data minimization rules to effectively protect consumer privacy.[45]

Another strong privacy and consumer protection framework are the rules issued by the CFPB to implement Section 1033 of the Dodd-Frank Act.[46] These rules include 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.[47] While the CFPB has said it will be revisiting its Section 1033 rule, we hope and will advocate with the Bureau that the rule retain these best-in-class privacy protections.

EPIC and U.S. PIRG Education Fund recently published a report evaluating the effectiveness of state privacy laws.[48] The report states that a strong, effective consumer privacy law would do the following:

- impose data minimization obligations on companies that collect and use personal information – taking the burden off of individuals to manage their privacy online and instead requiring entities to limit their data collection to better match consumer expectations;

[44] *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/.
[45] *Id*.
[46] 12 C.F.R. Part 1033.
[47] *Id.*
[48] Caitriona Fitzgerald, Kara Williams, and R.J. Cross, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC & U.S. PIRG Education Fund (Jan. 2025), https://epic.org/state-of-privacy-2025.

- strictly regulate all uses of sensitive data, including health data, biometrics, financial data, and location data,
- require that companies obtain meaningful opt-in consent from consumers before transferring their sensitive data, including for targeted marketing;
- ban the sale of sensitive data;
- establish strong civil rights safeguards online and rein in harmful profiling of consumers;
- provide consumers with rights such as the right to access, correct, and delete their personal data and require companies to have procedures to ensure the accuracy of data;
- prohibit companies from discriminating against consumers for exercising their privacy rights;
- provide strong enforcement and regulatory powers to ensure the rules are followed; and
- enable consumers to hold companies accountable for violations in court.[49]

Any general privacy law at the state or federal level should include these elements to ensure that the law provides meaningful privacy protections, empowers consumers to exercise their privacy rights, and limits the ability of companies to perpetuate data-driven harms. Congress should include these elements in federal privacy legislation to effectively protect the privacy and data security of American consumers.

Response to Question 11: Should we consider requiring consumers be provided with a list of entities receiving their data?

Currently, consumers often have no idea how their data is collected, sold, and shared. The privacy policies provided to consumers by companies generally include vague information about all of the types of data that may be collected, sold, and shared. However, the policies fail to give consumers clear notice about the specific data points collected and stored by the company, the specific information that is sold or shared with third parties, and the specific entities to which data is sold or shared. Companies that sell consumer data to third parties should be required to provide clear, specific, concise, up-to-date notices to consumers regarding the data held by the company and the data shared with third parties, including a list of the specific entities that received personal data.

[49] *Id.*

Providing transparency to consumers about how their data is shared or sold is necessary, but it is not sufficient to protect consumer privacy. As explained in response to Question 1, strong data minimization standards, which only permit companies to collect and use personal data when doing so is necessary to provide the product or service the consumer requested provides, are necessary to ensure consumer privacy. Companies should not be permitted to collect and use personal data however they please simply because they disclosed they were doing so in a long privacy notice. The Committee should work to increase transparency for consumers about how their data is disclosed to other entities, but it must also work to ensure that consumers have substantive privacy rights and are empowered to exercise their privacy rights.

Response to Question 12: Should we consider changing the structure by which a financial institution is held liable if data it collects or holds is shared with a third-party, and that third-party is breached?

The GLBA does not currently include provisions holding financial institutions liable to consumers for violations, but it should. Financial institutions also have obligations under the Electronic Fund Transfer Act (EFTA) and the Truth in Lending Act (TILA) to protect consumers from liability for unauthorized transfers, which in some cases may be related to data breaches. We have no opinion on whether financial institutions should be able to pursue third parties if they believe that those third parties caused the financial institution to suffer a loss, so long as consumers are held harmless and retain their right to dispute charges directly with their financial institution.

Congress should amend the liability provisions of the GLBA by empowering consumers to seek relief when their rights under the Act are violated, *i.e.*, there should be a private remedy for consumers to enforce the GLBA. The GLBA's lack of a private remedy is one of the fundamental deficiencies of the Act. In numerous legal cases, consumers who believed that financial institutions had violated their rights under the GLBA were denied the ability to seek redress in a court of law.[50]

[50] *See generally*, National Consumer Law Center, Fair Credit Reporting (10th ed. 2022) § 18.4.1.12, updated at www.nclc.org/library (collecting cases).

This lack of private enforceability renders the Act of little practical value to those who seek to limit, or even monitor, the use of their own personal data.

Enforcement of the GLBA is limited to a handful of federal agencies, such as the CFPB, Federal Trade Commission, federal banking regulators, the Securities and Exchange Commission, and only one set of state agencies, *i.e.,* state insurance regulators.[51] In the best of times, these agencies must balance pursuing GLBA violations against all of the other competing demands for their limited resources to enforce other consumer protection laws. This has been exacerbated now by the wide-scale firing of staff and gutting of regulatory oversight at the CFPB, and by similar reductions in capacity of other federal regulators. Given current federal capacity, violations of the GLBA will likely go unenforced. Even for those who favor less agency regulation, allowing individuals to seek remedies when a company violates the law is a way of promoting the rule of law in a free market. Strengthening GLBA protections without strengthening its remedies would not be adequate to meaningfully protect consumers.

The EFTA and TILA both have private rights of action, but neither the EFTA nor TILA directly address data breaches. However, financial institutions have a duty to protect consumers from liability for unauthorized transfers from their accounts, and sometimes those unauthorized transfers are made possible by information exposed in a data breach.

When a bank account or credit card has an unauthorized charge, both the EFTA and TILA give the consumer the right to dispute that charge with their financial institution and require the financial institution to follow dispute resolution processes that include reimbursing the consumer if the charge was, in fact, unauthorized. That obligation must remain unchanged and vigorously protected. It is typically impossible to know if a given unauthorized charge is traceable to a particular data breach, and consumers certainly have no way of knowing that. Financial institutions also have obligations to ensure the safety of accounts and prevent unauthorized access even, or especially, in a world where a lot of information is exposed in data breaches.

[51] 15 U.S.C. § 6805(a).

Consumers also need to know where to go when an unauthorized charge has been made. When their bank account has an unauthorized charge, they must be able to go to their bank. When their credit card has an unauthorized charge, they should be able to seek relief from their credit card company. If the financial institution believes that an unauthorized charge is traceable to a data breach at a third party, it can pursue that third party. But it would be completely unworkable and would expose consumers to devastating losses if financial institutions could escape their EFTA and TILA duties simply by claiming that the loss was a third party's fault.

Response to Question 13: Should we consider changes to require or encourage financial institutions, third parties, and other holders of consumer financial data to minimize data collection to only collection that is needed to effectuate a consumer transaction and place limits on the time-period for data retention?

Yes, as recommended in response to Questions 1 and 8, Congress should pass comprehensive privacy legislation that includes strong 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.[52] Companies should not be permitted to siphon up consumer data without limits, use the data however they wish, sell the data willy-nilly to third parties, and retain the data as long as they want. The majority of state and federal privacy laws allow just that, simply requiring companies to disclose their privacy practices in Terms-of-Use agreements and privacy policies. The notice-and-choice model, also discussed in response to Question 1, incentivizes companies to include long, vague, and broadly worded lists of scenarios in which they may collect consumer data in their privacy policies.[53] In doing this, companies provide themselves legal cover to collect data in any way they may wish in

[52] *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/.)

[53] *See The State of Privacy 2025: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better,* EPIC and U.S. PIRG Education Fund (Jan. 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-PIRG-State-of-Privacy-2025.pdf.

the future.[54] If consumers object to any of the terms, their only choice is not to use the service at all. Especially in the context of financial services, this illusion of "choice" is particularly stark because financial services are essential to consumers. People need access to financial services like banking and credit to function in modern society, so consumers do not have a real choice to not use financial services if they object to the privacy policies.

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. Data minimization, opt in requirements for selling/sharing/targeted marketing, anti-discrimination requirements, accuracy and error resolution provisions, and meaningful remedies are necessary to effectively protect the privacy and data security of all consumer data, and financial data is no exception.

Sincerely,

/s/ Caroline Kraczon
Law Fellow
Electronic Privacy Information Center

/s/ Alan Butler
Executive Director
Electronic Privacy Information Center

/s/ Chi Chi Wu
Director of Consumer Reporting and Data Advocacy
National Consumer Law Center

/s/ Carla Sanchez-Adams
Senior Attorney
National Consumer Law Center

[54] *Id.*