U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

August 28, 2025

The Honorable French Hill
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Andy Barr
Chairman
Subcommittee on Financial Institutions
U.S. House of Representatives
Washington, DC 20515

VIA ELECTRONIC SUBMISSION

Re: **House Financial Services Committee Request for Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals**

The Chamber respectfully submits comments to the House Financial Services Committee on its request for comments on current and potential data privacy laws.[1] For consumers to reap the benefits of the digital economy and to ensure consistent privacy protections, the Chamber advocates for strong preemptive privacy legislation that prevents a patchwork of laws from creating confusion and inhibiting innovation. At the same time, we recognize that financial institutions have already been covered by Gramm-Leach-Bliley Act ("GLBA") obligations for nearly a quarter century. In keeping with the need for uniformity and current laws, we offer the following responses to questions posed by the Committee.

1. Should we amend the Gramm-Leach-Bliley Act (GLBA) or consider a broader approach?

Updating the existing GLBA is the targeted and preferred approach. While there is room to improve the broader framework by updating certain practices and clarifying key terms and compliance standards, the GLBA has proven to be a suitable framework for financial privacy for over 25 years.

Focusing on amending the GLBA not only would provide a strong foundation for modernizing provisions that need updating but would also allow for better harmonization with existing state provisions. For example, the NAIC developed Model #672 to implement the GLBA's standards for how insurance companies collect, use,

[1] *See* Press Release, "House Financial Services Committee Requests Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals," (July 31, 2025) *available at* https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=410833.

and disclose consumer personal information. Today Model #672 is a great success, largely integrated into most states through the process of implementing the GLBA (and as a practical matter, all states have these requirements in place).

2. Should we consider a preemptive federal GLBA standard or maintain the current GLBA federal floor approach?

To facilitate the development of innovative financial products and services, Congress should pass a fully preemptive privacy law that a) eliminates a patchwork of state laws and b) prevents States from evading the intent of Congress by drafting laws that survive preemption in the future. When amending the GLBA, Congress should work to achieve these goals. Simply adopting a national privacy law without strong preemption would enable a state patchwork of laws that will be confusing to both consumers and potentially impossible for small businesses to comply with. To be clear, we are proposing both of the following: (a) a federal privacy law (that exempts GLBA activity) that fully preempts state privacy law; and (b) a GLBA that fully preempts state laws in this area.

A 2022 report from ITI highlighted that a national patchwork of privacy laws would cost the United States economy $1 trillion and disproportionately impact small businesses with a $200 billion economic burden.[2] Most small businesses are worried a patchwork of state laws will increase litigation and compliance costs.[3]

To achieve the goal of strong preemption, a national privacy law must explicitly state that it preempts or supersedes all state privacy laws and regulations *related to* data privacy and security. Recent legislation like the American Privacy Rights Act fell short of providing this needed language by, instead, merely proposing to preempt what was *covered by* the national privacy law.

To provide the strongest preemption, according to a Congressional Research Service report, Congress should use much stronger language than "covering" or "covered by".[4] According to the Supreme Court, "'covering' is a more restrictive term which indicates that pre-emption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[5] Similarly, under a "covered by" approach, Congress would have to draft within a national privacy law all the different

---

[2] ITIF, "The Looming Cost of a Patchwork of State Privacy Laws," (January 2022) *available at* https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.

[3] U.S. Chamber of Commerce, "Empowering Small Business: The Impact of Technology of U.S. Small Business Fourth Edition" (August 2025) *available at* https://www.uschamber.com/assets/documents/20251621-CTEC-Empowering-Small-Business-Report-2025-v1-r10-Digital-FINAL.pdf.

[4] Congressional Research Service, "Federal Preemption: A Legal Primer" (2023) *available at* https://www.congress.gov/crs_external_products/R/PDF/R45825/R45825.3.pdf.

[5] *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 663 (1993).

state obligations and requirements before they can arguably be preempted. Such an approach also does not account for the future laws passed by states that may not match the requirements of the federal laws.

We would also encourage Congress to refrain from including excessive exceptions to preemption that could be interpreted by courts as language showing Congress did not intend for there to be strong preemption. For example, Congress should avoid carving out from preemption any biometric[6] or broad health privacy laws.[7] At the same time, privacy legislation should not broadly preempt against laws of general applicability like state consumer protection and civil rights laws, so long as the underlying claim is not based on a privacy violation.

Former Chairman McHenry's legislation, introduced in the 118th Congress, included helpful language on preemption.[8] The federal standard would be the operative standard. Specifically, the Data Privacy Act's Section 7 would have amended Section 507 [Relation to State Laws] to make clear that the GLBA supersedes any statute or rule from a state that regulates a Financial Institution's collection and disclosure of data, privacy notices, data breach notifications, access, deletion, or other rights, and international sharing. This is more finite and ideal for a single compliance standard.

A general federal preemption of state laws touching on privacy issues, such as the laws like the California Consumer Privacy Act, would simplify compliance requirements (reducing costs), facilitate competition, and stimulate innovation and business growth in the increasingly borderless US economy.

3. If GLBA is made a preemptive federal standard, how should it address state laws that only provide for a data-level exemption from their general consumer data privacy laws?

If the GLBA is modernized and made fully preemptive by federal standard, the state provisions that regulate in this area will be preempted. So long as federal legislation is truly preemptive, the harmonization with existing GLBA provisions in states should be seamless. For states that have lesser exemptions in state privacy laws, they will have to rise to the level of a GLBA exemption in a federal bill, ideally an entity and affiliate level exemption.

4. How should GLBA relate to other federal consumer data privacy laws, both a potential general data privacy law and current sector-specific laws?

---

[6] *See e.g.* 740 ILCS 14/1.

[7] *See* RCW § 19.373.005 *et al.*

[8] Data Privacy Act *available at* https://www.congress.gov/bill/118th-congress/house-bill/1165.

The Chamber supports comprehensive privacy legislation with GLBA preemption. We support an updated GLBA to fully preempt state laws that regulate GLBA activity.

5. How should we define "non-public personal information" within the context of privacy regulations?

"Non-public personal information" in the GLBA context should remain as it is currently defined.

"Publicly available data" should be defined to include both data contained in publicly available records and other data reasonably believed to be accessible to the public.

Data should not be subject to the new law when it has been de-identified. The definition of de-identified should apply to any data that does not identify or is not associated with an individual and could not reasonably be used to identify an individual.

6. Do the definitions of "consumer" and "customer relationship" in GLBA require modification?

The GLBA's requirements differ between when an individual is a consumer and when a customer relationship is formed. Accordingly, for now we support maintaining these distinctions.

7. Does the current definition of "financial institution" sufficiently cover entities that should be subject to GLBA Title V requirements, such as data aggregators?

The Chamber strongly supports passage of a general comprehensive privacy law that protects all Americans, as well as amendments to the GLBA. We express concerns about expanding the definition of covered "financial institutions" that would create regulatory overlap with a new general data privacy and protection law.

8. Are there states that have developed effective privacy frameworks?

Twenty States have passed comprehensive privacy legislation with seventeen adopting the Consensus Privacy Approach which has been adopted in states like Virginia and Kentucky. The Chamber supports a general national data privacy law based upon the protections afforded consumers in this Consensus Privacy Approach[9]. These statutes were not specifically written for the financial services industry and, in fact, often exempt financial institutions altogether. Nevertheless, some of these new laws do include elements that should be included in an updated GLBA. For example,

[9] *See* Comments of U.S. Chamber to House Privacy Working Group (April 7, 2025) *available at* https://www.uschamber.com/assets/documents/250401_Comments_House-Privacy-Working-Group_EC.pdf.

the Virginia Consumer Data Protection Act ("VCDPA") includes a flexible approach to drafting and delivering privacy notices electronically (e.g., posted publicly on a website) and a clear exclusion of any private right of action.

There are concepts in existing state frameworks that have proven to be successful in both striking a balance in consumer protections and availability of products to consumers. These provisions, taken in the context of their corresponding definitions and other language within the same law, can serve as an initial example of appropriate regulation.

Reasonable Time Periods

Concepts in VCDPA Section 38.2-600 include reasonable time periods for consumers to request correction, amendments, or deletion of information, appropriate opportunities for challenges to this information, and appropriate access limitations to health information.

Access

If the Committee elects to adopt the Consensus Privacy Approach and require data portability, it would be helpful if the right can only be exercised by the consumer, and applied only to data provided by the consumer. This would mean that any secondary or derived data wouldn't need to be delivered to a third party.

De-identified information

The Committee could leverage the VCDPA, which explicitly excludes de-identified data from the definition of personal data and provides a reference standard, which might be helpful to reference as well.

Deletion

The Consensus State Approach also provides consumers the ability to delete data. In order to strike the right balance of consumer protection and beneficial uses of data, the Committee should consider the VCDPA's exemptions to this right. Specifically, the VDCPA:

1. Provides the ability to maintain records for other legal requirements.[10]
2. Requires permanently and completely erasing apart from archiving or back-up—this is an important exception since we are obligated to archive. Many laws don't articulate this.
3. Allows for deidentifying or aggregating the data as an alternative to deletion. It is also important that any proposed language includes clear exemptions—especially for publicly available information and data used for fraud prevention.

[10] *See* VCDPA Section 59.1-579(B)(2).

9. Should we consider requiring consent to be obtained before collecting certain types of data, such as PIN Numbers and IP addresses?

Financial institutions should not be required to obtain consent for the collection and use of information reasonably necessary to provide a financial product or service and for other important purposes such as fraud prevention. Processing data elements like PIN numbers, IP addresses, and other data is reasonably necessary, especially for fraud prevention and information security purposes, and is protected by existing information security standards.

10. Should we consider mandating the deletion of data for accounts that have been inactive for over a year, provided the customer is notified and no response is received?

No. Regulated financial institutions are subject to prescriptive record retention requirements that make such an approach impractical to implement. For example, this sort of mandate can disproportionately impact life insurers who collect this information for longer periods of time than other businesses. While the notification to the customer may seem sufficient, for life insurance companies there have been examples where this data is proven to be beneficial to customers. If any provision is added to draft legislation, the unique position of life insurers should be considered and exempted from this type of mandate. In addition, a mandate of deletion of data for accounts inactive for over a year conflicts with other state and federal regulatory requirements and may be technically infeasible given these other requirements where records are stored in certain formats for regulatory purposes.

11. Should we consider requiring consumers be provided with a list of entities receiving their data?

No. This would be impractical to implement and raise security risks. Financial institutions often have hundreds of service providers who process on behalf of the institution non-public personal information. In addition, those service providers change from time to time, requiring frequent updates that would likely not be useful to individual customers and consumers. Such an approach would also increase security risks by providing hackers and other threat actors a list of service providers that could be subject to coordinated attacks.

Sharing a list of entities would be lengthy in nature, could require approvals from such third parties, and, chiefly, could cause an information security vulnerability given the public is aware of the third parties where data is stored. Providing categories of service providers with whom customer information is shared is far more useful than the exact entities. Categories have been used in nearly all states and are understood

by consumers as the norm. For example, providing the name XYZ in a list would not allow the customer to understand the purpose of the information-sharing. It would be more beneficial to customers to know that their information was shared with a service provider that provides security services instead of a company name that they might not understand. Financial institutions understand their obligations to safeguard customer information.

Such an approach would also conflict with the Consensus Privacy Approach, which only requires the disclosure of categories—not all entities—of third parties to consumers.

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?

Entities under the GLBA should retain their current regulators. For example, in the insurance context, it may be appropriate to recognize the state-level regulators who monitor the sector.

Businesses should be given a reasonable opportunity to cure violations of the law before enforcement actions can be taken. Additionally, since security standards are constantly evolving to protect consumers, Congress should consider including a safe harbor provision that offers an affirmative defense for entities complying with established security standards.[11]

Federal privacy legislation should follow the Consensus Privacy Approach by stating that nothing in the law "shall be construed as providing the basis for, or be subject to, a private right of action for violations…under any other law."[12]

Data protection legislation should avoid empowering the private trial bar at the expense of business innovation and viability. Frivolous litigation, not based on harm to consumers, has been used in the past to extract costly settlements from companies, even small businesses, based on privacy law provisions granting a private right of action. In particular, private rights of action are ill-suited in privacy laws because:[13]

- They undermine appropriate agency enforcement and allow plaintiffs' attorneys to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who can be expected

[11] *See e.g.* Tenn Code Ann. § 47-18-3213.
[12] Va. Code Ann. § 59.1-584(E).
[13] U.S. Chamber Institute for Legal Reform, "Ill-Suited: Private Rights of Action and Privacy Claims," (July 2019) *available at* https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf.

to understand the complexities of encouraging compliance and innovation while preventing and remediating harms.

- They can lead to a series of inconsistent and dramatically varied district-by-district court rulings. Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all American consumers and provide structure for companies aiming to align their practices with existing and developing law.
- They, combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, are routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionately benefit plaintiffs' attorneys
- Rather than individuals whose privacy interests may have been infringed. This may force businesses to focus their resources on defending this time-consuming and expensive private litigation rather than towards compliance with the law and protecting consumer rights.
- They hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies.

Private rights of action would be particularly devastating for business under a privacy law that does not have a strong preemptive effect. Not only would states be able to continue passing their own laws, but individual judicial district precedent could also create further confusion and conflict.

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?

Data minimization is critical to safeguarding consumer privacy and security. At the same time, data minimization standards that are too strict could impede innovation and the ultimate goal of protecting people and systems. States that have passed the Consensus Privacy Approach have enacted a balanced and workable data minimization standard.

For example, states like Virginia, Kentucky and Texas mandate companies limit data collection to what is "adequate, relevant, and reasonably necessary" related to a *disclosed* purpose.[14] By contrast, states like Maryland have enacted stricter data minimization requirements that only allow the collection or processing of data for "what is necessary and proportionate to provide or maintain a specific product or

[14]Tenn. Code Ann § 47-18-3208(a)(1); Tex. Bus. & Com. Code Ann § 541.101(1) (emphasis added).

service requested by the consumer to whom the data pertains."[15] Congress should avoid approach taken by Maryland which further imposes a restriction that prohibits the collection or processing of sensitive data - even with consent - unless it "is strictly necessary to provide or maintain a specific product or service..."[16]

Such a strict data minimization approach could limit companies' ability to use personal data for important purposes such as anti-fraud protections, Know Your Customer, and other web-based security applications (used by federal programs to reduce theft of benefits and identity fraud). Data has also enabled law enforcement to stop criminal activity such as human trafficking and organized crime.[17]

Finally, strict data minimization standards are threatening to create conflicting regulations in states. For example, Colorado's new AI law imposes liability on AI developers and deployers who fail to take reasonable care to prevent "unlawful differential...impact" that disfavors individuals or groups on the basis of certain protected classes like race and gender.[18] Many of these protected categories align with definitions of sensitive personal information in privacy laws. Strict data minimization laws would deprive companies of the data necessary to comply with other laws like state AI and anti-discrimination requirements.

We look forward to working with you to ensure that privacy laws are modernized in a way that enables businesses to continue seamless transactions, ensures innovation continues, and protects consumers while preventing a patchwork of state laws. If you require more information, please contact me at jcrenshaw@uschamber.com.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

[15] Md. Code Ann. Comm. Law § 14-4606(B)(1)
[16] *Id.* at § 1404607(A)(1).
[17] Chamber Technology Engagement Center, "Data For Good: Promoting Safety, Health and Inclusion" (January 2020) *available at* https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf.