GLBA Set for Overhaul? 10 Questions That May Decide the Next Generation of Financial Privacy Law

Insights
8.18.25

Congress is asking the financial industry – and anyone else with a stake in consumer data – to weigh in on the future of the Gramm-Leach-Bliley Act (GLBA). On July 31, the US House Financial Services Committee leaders issued a request for public comment to answer a series of key questions that could drive the first major overhaul of the nation's primary financial privacy law in more than 25 years. The review comes as fintech growth, state-by-state privacy patchworks, and new technologies like AI are challenging whether the GLBA still delivers the protections it promised. What do stakeholders, industry leaders, and the general public need to know before sharing their views on the future of federal consumer financial data privacy?

Background of the GLBA

Enacted in 1999, the GLBA is the cornerstone federal law governing the privacy and security of consumer financial information. At the time it was enacted, it was a monumental shift in the obligations for financial institutions with respect to how those entities handled personal information. And that includes more types of businesses than you might think, as the statute covers car dealerships, payday lenders, debt collectors, some retailers, tax preparers, travel agents, and more.

Now, more than 25 years later, the Committee is seeking public feedback on potential changes to the GLBA. This call for input signals the need for reform given the confounding landscape of consumer privacy laws at both the state and federal level.

Why Revise the GLBA?

Both the technology and legal landscapes have evolved dramatically since Congress passed the GLBA in 1999. The GLBA may no longer be up to the task of protecting consumer's personal information given the tremendous increase in fintech firms, data aggregators, website tracking, mobile apps for consumer financial services, and the AI implications for financial services.

Moreover, numerous states have passed consumer privacy laws that have complicated the picture. While most have exempted entities subject to GLBA, some like California have only exempted data subject to GLBA. Other states, like Connecticut, are rolling back the entity-level exemptions, creating a complicated matrix of laws applying to subsets of data and entities.

10 Key Questions Under Consideration

Lawmakers believe that less complexity in the legal framework may be needed, while at the same time adding more robustness when it comes to consumers' financial data. In order to determine the next steps when it comes to possible reform, Congressional leaders have asked interested members of the public to send their comments related to these (and other) questions by August 28.

1. Is amending GLBA alone sufficient?

While amending the GLBA is important, that alone may not suffice. A broader, comprehensive federal data privacy law could harmonize protections across sectors and states, offering a more uniform standard. A revised GLBA could even be incorporated into updates for other federal sector specific privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA). Despite numerous attempts, a federal consumer privacy law has yet to pass.

2. Will we ever get a consensus on the issue of preemption?

The perennial issue of preemption is the stumbling block. Having a federal law that preempts the proliferation of state consumer privacy laws could provide a much-needed streamlined approach for businesses and uniformity for consumers. However, it may also weaken strong state level protections in nearly half the states. Rolling back consumer privacy rights seems ill-advised given the overwhelming concerns over emerging technologies.

3. Should Congress expand the definition of "personally identifiable financial information"?

Expanding or modernizing the definition of "personally identifiable financial information" to cover digital identifiers, such as IP addresses, geolocation data, and behavioral analytics, as well as inferences, could strengthen protections and align the GLBA with modern data practices, addressing gaps that state laws are often called upon to regulate.

4. Is it time to retire the distinction between a "consumer" and a "customer"?

Updating these terms to reflect today's more transient financial relationships (e.g., platform-based interactions, non-traditional lending, robo-advisors) would help ensure the law applies uniformly across both traditional and emerging financial models. That could also provide equal protections for all data through a broader definition of non-public personal information.

5. Should we expand the scope of what constitutes financial information?

As non-traditional entities like fintech apps and data aggregators increasingly handle sensitive financial data, extending GLBA's scope to include them under Title V would fill regulatory gaps and ensure more consistent protections across all handlers of consumer financial information.

6. Does the GLBA need to offer consumers rights with respect to their data?

A potential approach is to incorporate consumer rights, such as data access, deletion, and opt-out rights, borrowing specific elements from state privacy laws. This might make preemption more appealing to certain states and consumers. However, data deletion rights may have limited applicability, as many entities are legally required to maintain certain, although not all, information.

7. Is it time for the GLBA to have more stringent requirements for "Sensitive Data"?

Mandating consent before collecting or sharing sensitive identifiers (e.g., social security numbers, and PINs, specific geolocation data) would align the GLBA with broader consumer expectations around transparency and control. The GLBA could also differentiate "sensitive personal information" from other types of data, bringing it more into alignment with some of the existing state consumer privacy laws.

8. Do financial institutions need to have more incentive to minimize and delete data?

Requiring data minimization and reducing retention periods would improve data security risks. However, that valuable option must be weighed against the need of financial institutions to defend themselves and demonstrate other aspects of regulatory compliance. While deleting outdated data can lower breach risks, implementation would require safeguards for financial institutions to meet other obligations (e.g., fraud detection, audit trails).

9. Should the GLBA require expanded disclosure of financial institutions data-sharing practices?

The GLBA's current disclosure requirements regarding data-sharing are very limited. Expanding the definition of "sharing," increasing disclosure obligations, as well as granting consumers the right to limit such sharing would create a significant alignment between the GLBA and state consumer privacy laws.

10. Does the GLBA need to strengthen its data security protections – and is a private right of action necessary in order for financial institutions to comply?

The GLBA does not have a private right of action. The inclusion or exclusion of a private right of action has been a point of contention in several attempts to pass a comprehensive federal privacy law. Allowing consumers to sue could incentivize stronger protections and create better oversight of third-party vendors. However, it would also increase operational costs and legal exposure for financial institutions. The question remains whether this would increase the security for consumers' data or simply increase costs.

Conclusion

Financial institutions, consumer advocates, privacy experts, and technology firms should seize this opportunity to contribute feedback. The outcome could become the master plan for the next generation of financial data privacy regulation in the United States. Consider reaching out to the FP Advocacy team to help develop best strategies for having your voice heard before the comment period expires on August 28.

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. You can also visit FP's US Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group, Consumer Privacy Team, or Financial Services Industry Team.

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301
Email

Xuan Zhou, CIPP/US, CIPM, CIPP/E
Associate
858.597.9632
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Industry Focus

Financial Services

Trending

U.S. Privacy Hub