Joint Financial Trades Response

House Energy & Commerce Committee

Request for Information

Data Privacy

April 4, 2025

Chairman Guthrie and Vice Chairman Joyce, we appreciate the opportunity to respond to the Committee and the Data Privacy Working Group's Request for Information on the parameters for a federal, comprehensive data privacy and security framework.

Our members have been, and continue to be, strong proponents for the protection of consumer data and privacy. Unlike many other businesses, our members consider the protection of consumer financial data to be a cornerstone of their business. This commitment to the protection of consumer financial data predates when Congress first began enacting data privacy laws in the 1970s, with the enactment of the Fair Credit Reporting Act ("FCRA") and the Right to Financial Privacy Act ("RFPA"). Our members have been subject to extensive federal privacy and data protection laws and regulations for almost half a century. We support privacy and data security protections for consumer data for other companies who have not been subject to robust laws and oversight on the protection of consumer data.

Summary

Our organizations support legislation to protect consumer privacy that:

- Establishes a national privacy standard that recognizes that strong privacy and data security standards are already in place for financial institutions under the Gramm-Leach-Bliley Act ("GLBA") and other financial privacy laws and avoid provisions that duplicate or are inconsistent with those existing laws.

- Eliminates the current inconsistent patchwork of state privacy, data security, and Artificial Intelligence ("AI") laws. A national standard containing these elements would provide consistent protection for consumers regardless of where they may live;

- Provides robust, exclusive enforcement of this national standard by the appropriate federal or state regulators, including preserving GLBA's existing administrative enforcement structure for financial institutions; and

- Consistent with the recommendation of the House Bipartisan Task Force on Artificial Intelligence,[1] recognizes the risk management framework set by federal banking regulators for AI that are already in place for banks and credit unions, as well as the relevant associated examination of banks and credit unions by their federal prudential regulators for compliance with such requirements, avoiding any duplicate or inconsistent regulation.

GLBA: Data Security and Privacy

The primary privacy and data security consumer protection law to which financial institutions are subject is Title V of the GLBA. The GLBA represented the first time that Congress enacted sector-specific, comprehensive privacy and data security standards, in this first instance for financial institutions and consumer financial data. With the GLBA, Congress carefully constructed a privacy and data security regime that provides consumers with meaningful privacy rights, while also ensuring that consumers can conduct financial transactions seamlessly and safely regardless of where they live and ensuring that financial institutions can, for example, protect against fraud, illicit finance, money laundering and terrorist financing.

Further, the GLBA provides various federal financial regulators with meaningful authority to adopt regulations to implement robust privacy and data security standards. This has allowed the regulatory regime to be flexible and adapt over time as privacy considerations evolve. In addition, federal financial regulators generally examine financial institutions for their compliance with privacy and data security requirements and have the authority to bring enforcement actions against those institutions that are found to be out of compliance with these requirements.

Notably, the GLBA requires that financial institutions provide consumers with notice relating to their collection and handling of consumer data and with information about their privacy and data security practices. Significantly, the GLBA prohibits a financial institution from disclosing information relating to a consumer to a nonaffiliated third party, unless the consumer is provided with notice and an opportunity to opt out of such disclosure and does not opt out or an exception applies permitting the disclosure (*e.g.*, to process a transaction, prevent fraud, with the consumer's consent, to comply with applicable law). Moreover, the GLBA and its implementing regulations impose substantive obligations to put security controls in place to protect consumer information and, in many instances, provide consumers with notice of security incidents involving sensitive information. Ultimately, Congress has long recognized the importance of privacy for financial institutions and has put in place meaningful privacy and security protections, carefully balanced with common sense exceptions to minimize disruptions to financial markets, transactions, and accounts.

While the financial services trade associations support legislation to establish a national privacy standard, that standard must recognize the strong privacy and data security standards that are already in place for the financial sector under the GLBA and other financial privacy laws and must avoid provisions that duplicate or are inconsistent with those laws.

[1] *Supra* note 2.

The Committee considered data privacy legislation in the 118th Congress, which included an exception for institutions covered by GLBA. The language, however, was ambiguous and did not clearly exempt financial institutions from the requirements of the bill. This would have led to duplicative and conflicting requirements for financial institutions already subject to the GLBA and oversight by the financial regulators. Ultimately, this framework would have been disruptive to the financial system, consumers, and the economy, and we advocated that it should be amended to exempt all financial institutions to avoid such disruption.

Preemption of State Law

The increasing patchwork of state privacy, data security, automated decision-making and laws must be replaced by a federal standard. In our view, it is critical that any new federal privacy law preempt existing state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial markets, transactions, and accounts. Moreover, a federal standard would ensure that consumers receive the same privacy rights and data protections regardless of where they may live.

Although legislation considered by the Committee in the 118th Congress would have preempted many state laws, it also included numerous exceptions that would have undermined its preemption, including specifically preserving several highly litigated state privacy laws. In essence, it would have codified a patchwork of state privacy laws. Data privacy legislation should create clear and direct preemption of all state privacy and data protection provisions to prevent the continued patchwork of requirements imposed on companies.

Enforcement

As noted, one of the most important elements of any federal privacy legislation is assurance and clarity that the legislation will be consistent from state-to-state. A uniform national standard is the foundation for adopting federal privacy legislation. If legislation allows enforcement by private rights of action, however, it will only be a short matter of time before different judicial interpretations result in different standards applying in different states (*e.g.*, a consumer in Nebraska will have different privacy protections than someone in Alabama). Another disadvantage is that these state-by-state variations inhibit national training and consumer understanding of privacy rights.

Further, a private right of action in this context will only serve to encourage frivolous litigation from plaintiffs' attorneys and will further encourage class actions even for minor compliance infractions. As in many class action suits, companies are forced to settle to avoid outrageous litigation costs even if the firm is not at fault. As such, our members do not support provisions, such as those included in legislation considered by the Committee in the 118th Congress that would authorize private rights of action.

For our members, it is very important that data privacy legislation provides robust, exclusive enforcement of this national standard by the appropriate federal or state regulators, including preserving GLBA's existing administrative enforcement structure for financial institutions.

Use of AI

Privacy discussions have evolved to include the implications and use cases associated with AI, particularly the generative iteration which involves training with large data sets to create new content. States have already begun to create a patchwork of AI laws.

The financial services industry is already subject to an extensive supervisory and regulatory regime and risk management framework covering nearly all risks associated with AI, including fair lending and cybersecurity requirements. Also, federally regulated financial institutions are subject to supervision, examination, and enforcement of their use of any technology, including AI. For example, banks and credit unions are subject to model risk management guidance.[2]

The House Bipartisan Task Force on Artificial Intelligence has rightfully recommended a "sectoral approach […] to financial services regulation" that ensures "primary regulators" can "leverage their expertise."[3] For example, Federal Reserve Governor Michelle Bowman has explained that, in the case of banking organizations, the use of AI must comply with relevant laws governing fair lending, cybersecurity, data privacy, third-party risk management, and copyright, adding that "when AI is deployed in a bank, an even broader set of requirements may apply depending on the use case."[4] Governor Bowman also called for a "gap analysis to determine if there are regulatory gaps" and for enhanced "coordination both within each agency and among domestic regulators that play a role in the supervision and regulation of the financial system."[5] This call underscores federal banking regulators' attentiveness to challenges posed by emerging technologies in the banking industry, as well as their commitment to the ongoing development of sector-specific regulation.

Accordingly, any AI-specific laws (or provisions) must not duplicate or be inconsistent with requirements already applied to financial institutions. Further, as with privacy laws, there is an ongoing risk that states will adopt laws governing AI which will stifle innovation by imposing

---

[2] SR 11-7, OCC Bulletin 2011-12, FIL-22-2017, SR 21-8, OCC Bulletin 2021-19, and FIL-27-2021. The OCC also released a booklet for its examiners to use as an aid when supervising banks' model risk management programs; see https://www.occ.treas.gov/publications-and-resources/. With respect to credit unions, the NCUA makes references to the Federal Reserve's and OCC's model risk management guidance in its Examiner's Guide; see https://publishedguides.ncua.gov/examiner/Content/ExaminersGuide/SensitivityMarketRisk/EvaluatingIRR/Measurement/ModelRisk.htm.

[3] *Report on Artificial Intelligence*, Bipartisan H. Task Force on Artificial Intelligence, 118th Cong., at 240 (Dec. 2024), https://republicans-science.house.gov/_cache/files/a/a/aa2ee12f-8f0c-46a3-8ff8-8e4215d6a72b/6676530F7A30F243A24E254F6858233A.ai-task-force-report-final.pdf

[4] Gov. Michelle Bowman, *Artificial Intelligence in the Financial System*, Remarks, the 27th Annual Symposium on Building the Financial System of the 21st Century: An Agenda for Japan and the United States, FEDERAL RESERVE (Nov. 22, 2024), https://www.federalreserve.gov/newsevents/speech/bowman20241122a.htm.

[5] *Id.*

conflicting and unnecessary requirements on financial institutions. In some cases, these laws could impact the way many financial institutions have used AI for the last several decades. The Committee has a unique opportunity to preempt such state laws to ensure that US financial institutions remain competitive in the use and development of AI.

Conclusion

Our organizations support national data privacy legislation that:

- Recognizes the strong privacy and data security standards that are already in place for the financial sector under the GLBA and other financial privacy laws and must avoid provisions that duplicate or are inconsistent with those laws.

- Provides clear and direct preemption of all state privacy and data protection provisions to prevent the continued patchwork of requirements imposed on companies.

- Incorporates robust, exclusive enforcement of this national standard by the appropriate federal or state regulators, including preserving GLBA's existing administrative enforcement structure for financial institutions and does not include a private right of action.

- Does not duplicate or be inconsistent with AI requirements already applied to financial institutions.

We appreciate the opportunity to provide input to the Committee on this important issue and look forward to answering any questions about our views on this subject.

American Bankers Association
America's Credit Unions
Bank Policy Institute
Consumer Bankers Association
Independent Community Bankers of America
Mortgage Bankers Association
Securities Industry and Financial Markets Association