Statement for the Record

On Behalf of the

American Bankers Association

before the

Financial Institutions Subcommittee

of the

House Financial Services Committee

June 5, 2025

Statement for the Record

On Behalf of the

American Bankers Association

before the

Financial Institutions Subcommittee

of the

House Financial Services Committee

June 5, 2025

The American Bankers Association (ABA) appreciates the opportunity to provide a Statement for the Record for this hearing, "Framework for the Future: Reviewing Data Privacy in Today's Financial System." ABA is the voice of the nation's $24.5 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2.1 million people, safeguard $19.5 trillion in deposits and extend $12.8 trillion in loans.

Summary

ABA member banks strongly support the protection of consumer data and privacy and consider safeguarding 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. Consumers trust banks because they know their personal data is secure. Unlike other entities, banks are already subject to robust privacy requirements under the Gramm-Leach-Bliley Act ("GLBA"), in addition to other federal privacy laws. We support applying privacy and data security protection standards to other industries who have not been subject to robust laws and oversight on the protection of consumer data.

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. These privacy rights apply regardless of where customers live and ensure that financial institutions can 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 (a recent

positive example is a needed exception to the annual privacy notice).[1] 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.

Congress has also carefully balanced privacy protections with common sense exceptions to minimize disruptions to financial markets, transactions, and accounts. Any legislation to establish a national privacy 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—a new national privacy framework must avoid provisions that duplicate or are inconsistent with those laws.

Preemption of State Law

The increasing patchwork of state privacy, data security, automated decision-making and laws should 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. Any federal 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

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-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.

[1] https://www.federalregister.gov/documents/2018/08/17/2018-17572/amendment-to-the-annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p.

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 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 Artificial Intelligence

Privacy discussions have evolved to include the implications and use cases associated with artificial intelligence (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 are subject to model risk management guidance.[2]

Also, the House Bipartisan Task Force on Artificial Intelligence 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." 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.

---

[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/.

[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.

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 conflicting and unnecessary requirements on financial institutions. In some cases, these laws could impact on 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.

Section 1033

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (P.L 111-203) requires financial institutions to provide consumers with access to their financial data in electronic form.

Any regulation implementing Section 1033 must strictly adhere to the statutory text due to the myriad of privacy, security, and financial risks that may result. For instance, greater access to bank systems and customer data by third parties without proper controls could lead to scope creep, significant issues with respect to fraud and liability, and the monetization of personal information. We believe that access to customer data held at a bank should be governed by the GLBA to avoid inconsistent and potentially unintended consequences and strongly support extending GLBA-like protection for customer data when it leaves the bank and enters the data aggregation ecosystem. At a minimum, data aggregators and large fintechs should be subject to the same supervisory regime as banks to ensure consistent privacy protections are in place.

ABA has submitted extensive comments to the CFPB on its Section 1033 rulemaking. The rule is currently subject to litigation, with the CFPB having indicated it believes the extant version of the regulation to be "unlawful." Much of this legal scrutiny stems from the fact that the open banking ecosystem developed subsequently to the passage of the Consumer Financial Protection Act of 2010. Regardless of the inclusion of any provisions on data access rights, we urge that the bill include a sunset on the use of the technology known as "screen scraping," which raises significant privacy and data security concerns, and which moreover interferes with the bandwidth and latency of online banking portals.

Previous Legislation and ABA Recommendations

In the 118th Congress, the Committee considered data privacy legislation in the form of H.R. 1165, the Data Privacy Act of 2023. It would have amended Title V of the GLBA by adding new privacy rights, such as the right to access and delete certain information that the financial institution maintains about the individual.

ABA supported several aspects of the bill, including a meaningful preemption provision to the GLBA to ensure that the GLBA preempts state laws on privacy for nonpublic personal information, and the additional clarity about the application of the GLBA to data aggregators. ABA was also pleased that the bill left enforcement to the prudential regulatory agencies. Enforcement authority should not be given to either state Attorneys General or achieved through

private rights of action (PRA), which would lead to frivolous class action lawsuits that could bankrupt a smaller bank for even a minor, technical violation.

But, as we shared with the Committee, ABA had concerns about several other provisions. For example, there are extensive new notification requirements (including two new annual notices that will result in a proliferation of notices), significant limits on data use and collection, other new and confusing obligations that would be difficult to implement, and an overly broad definition of "consumer relationship" that would impose unnecessary burdens on banks especially community banks.

If the Committee considers moving forward on data privacy legislation it should focus on any regulatory gaps and adhere to the following principles:

• Recognize that strong privacy and data security standards are already in place for financial institutions under the Gramm-Leach-Bliley Act and other financial privacy laws and avoid provisions that duplicate or are inconsistent with those existing laws. These same standards should be applied to federal government entities that hold sensitive personal information, including the bank regulatory agencies as evidenced by the recent data breach at the OCC.

• Eliminate 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.

• Provide 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, recognize the risk management framework set by federal banking regulators for AI that are already in place for banks, 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 regulations.

• Regardless of the inclusion of any provisions on data access rights, include a sunset on the use of the technology known as "screen scraping," which raises significant privacy and data security concerns, and which moreover interferes with the bandwidth and latency of online banking portals.

Conclusion

ABA member banks strongly support protecting consumer data and privacy and consider it to be the cornerstone of their business. Consumers trust banks because they know their personal data is secure. Unlike commercial entities in other sectors, banks are subject to robust privacy requirements under the GLBA and other federal privacy laws. The ABA supports applying

consumer privacy and data security protection standards to additional who have not been subject to robust laws and oversight in the protection of consumer data.

Thank you once again for allowing us to provide these comments and we look forward to working with Members of the Subcommittee on this important issue.