Statement for the Record

On Behalf of the

American Bankers Association

before the

House Financial Services Committee

March 17, 2026

Statement for the Record

On Behalf of the

American Bankers Association

before the

House Financial Services Committee

March 17, 2026

The American Bankers Association (ABA) appreciates the opportunity to provide a Statement for the Record for this hearing, "Updating America's Financial Privacy Framework for the 21st Century." The ABA is the voice of the nation's $25.3 trillion banking industry, which is composed of small, regional and large banks that together employ over 2 million people, safeguard $20.1 trillion in deposits and extend $13.5 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, and consumers trust the banking industry because they know their personal data is secure. Unlike some other entities, banks are already subject to robust privacy requirements under the Gramm-Leach-Bliley Act ("GLBA"), in addition to other federal privacy laws. The ABA urges Congress to apply commensurate 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 (for

example, a needed exception to the annual privacy notice requirement).[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 or an exception applies permitting the disclosure (*e.g.*, to process a transaction, prevent fraud, with the consumer's consent, or 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, and automated decision-making 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 due to varying state law frameworks.

Enforcement

One of the most important elements of any federal privacy legislation is assurance that the legislation will be consistent from state to state: a uniform national standard must serve as 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 the application of divergent standards in different states (*e.g.*, a consumer in one state will have different privacy protections than a similarly-situated consumer in another state). 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 member banks, 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 the proliferation of artificial intelligence (AI), particularly the generative iteration which involves training with large data sets to create new content. States have already begun passing legislation that is resulting in a patchwork of state laws governing AI.

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] While related, privacy laws are not necessarily coterminous with AI-specific laws, and one of the considerations for the Committee as it explores modernizing the GLBA will be the extent to which AI is addressed.

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. The ABA supports extending GLBA-like protections for customer data when that data leaves the bank and enters the data aggregation ecosystem. At a minimum, financial data aggregators and large fintechs should

[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/.

be subject to the same supervisory regime as banks to ensure consistent privacy protections are in place.

The ABA has submitted extensive comments to the CFPB on its Section 1033 rulemaking. The rule is currently being reconsidered by the CFPB, with a new proposed rule to be issued at any point. Significant questions remain about the ultimate scope of Section 1033, compounded by 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 Congress to address the use of the technology known as "screen scraping," the practice scanning a website, collecting data and identifying patterns by mimicking user behavior (often by using consumer access credentials), and saving important information for later use. This practice raises significant privacy and data security concerns, and which moreover interferes with the bandwidth and latency of online banking portals.

Legislation and ABA Recommendations

As the Committee explores changes to the federal data privacy framework, the ABA respectfully urges that such legislation focuses on revising the GLBA to address any regulatory gaps and adhere to the following principles:

- GLBA is a carefully calibrated regime designed to avoid interference with core financial activities that benefit consumers and will continue to be the most appropriate vehicle to ensure data privacy for financial institutions;

- The House Financial Services Committee should play an essential role in discussions on federal privacy legislation given its expertise in financial services, including any discussion of amendments to GLBA (e.g., additional data subject rights with appropriate exemptions and tailoring based on the unique fraud, security, and other risk considerations relevant to financial services);

- GLBA should strongly preempt state privacy laws; moreover entities, affiliates, and data subject to GLBA must be exempt from any comprehensive federal consumer privacy laws in order to avoid interference with the GLBA and important financial activities such as fraud prevention and underwriting;

- GLBA should continue to be enforced by federal regulators rather than through private litigation;

- GLBA should be amended to create a more consistent regulatory playing field among traditional and novel financial institutions as well as other entities operating in the financial ecosystem;

- GLBA should be amended to include a safe harbor for the sharing of information regarding fraud and scams; and

- GLBA should be harmonized with Section 1033 of the Dodd-Frank Act as appropriate, including to apportion liability for when consumer-permissioned data sharing results in a data breach as well as part of the data subject rights issue.

Data Privacy Draft Legislation. The ABA commends the Committee for releasing its March 12 Discussion Draft: "To make improvements to title V of the Gramm-Leach-Bliley Act and for other purposes." Our preliminary view is that the Discussion Draft incorporates many of the ABA principles highlighted above and provides a solid foundation for Congressional action. We are especially pleased that the draft includes strong preemption language and preserves the GLBA's existing regulatory and enforcement structure, while updating certain customer protections and taking into consideration potential regulatory impacts on community banks. We are currently reviewing the draft with our member banks and will provide our feedback on the draft legislation promptly to the Committee.

Conclusion

ABA member banks strongly support protecting consumer data and privacy and consider it to be the cornerstone of their business. We appreciate the Committee's engagement with the banking industry as it considers modernizing federal data privacy requirements. Thank you once again for allowing us to provide these comments and we look forward to working with Members of the Committee on this important issue.