BANK POLICY INSTITUTE

Testimony of Clara Kim

Bank Policy Institute Senior Vice President

Before the House Financial Services Committee

"Updating America's Financial Privacy Framework for the 21st Century"

March 17, 2026

Chairman Hill, Ranking Member Waters, and Honorable Members of the Committee, thank you for the opportunity to testify today. My name is Clara Kim, and I am a Senior Vice President at the Bank Policy Institute. BPI is a research and advocacy group supported by banks with more than $100 billion in U.S. assets. Collectively, our banks employ nearly two million Americans, make half of the nation's small business loans, and are an engine for economic growth. On behalf of BPI member companies, I appreciate the opportunity to discuss updating the U.S. financial privacy framework.

Financial institutions occupy a unique position in our economy. To keep the financial system safe and to serve customers effectively, banks must collect, use, and retain data in ways that are different from many other sectors. They have obligations under law to prevent fraud, money laundering, terrorist financing, and other illicit activity, and they rely on consumer financial data to do that work. This data is also necessary for other activities and services, such as underwriting a mortgage for a first-time homebuyer or extending credit in underserved communities. Many of these uses are mandated by statute or regulation or are fundamental to the safety and soundness of the financial system.

Data Privacy Under the Gramm-Leach-Bliley Act

In the decades since the Gramm-Leach-Bliley Act (GLBA) established federal privacy standards for financial institutions in 1999, many banking services have evolved from a strictly brick-and-mortar, face-to-face experience to an always-on, digital experience. But while the technology of banking has transformed since then, GLBA has consistently afforded consumers strong baseline privacy and information security protections, including notice, restrictions on sharing, and information security.

Banks operate under an extensive, comprehensive regulatory framework for privacy and data use. In addition to GLBA, banking organizations are subject to safety-and-soundness standards, third party risk management requirements, cybersecurity expectations, and other federal statutes such as the Fair Credit Reporting Act and the Right to Financial Privacy Act. These requirements are implemented and enforced through continuous, consolidated supervision by federal prudential regulators. That combination—GLBA-plus-prudential oversight—has produced a robust, sector-specific federal privacy regime that has worked for more than 25 years to protect consumers while allowing banks to perform their essential functions.

Updating Financial Data Privacy and the GLBA

The core principles of GLBA have worked well since it was established. In considering changes to the GLBA framework, it will be important to consider the potential for unintended consequences. GLBA was designed for financial institutions, with careful calibration between privacy protections and the legitimate, often legally required, uses of data that keep the system safe and inclusive. It has also proven adaptable: the federal regulators have updated implementing rules over time as technology, cyber threats, and consumer expectations have evolved. If Congress decides to move forward with GLBA modernization, we urge a focus on targeted amendments rather than a fundamental rewrite, to avoid disrupting the equilibrium that has developed across the many laws and regulations that govern how banks process and share data.

However, any entity that handles sensitive personal and financial data about consumers, including fintechs, data aggregators and crypto, should have to meet the same rigorous standards and duties as banks to protect that information. Banks operate under stringent information security requirements set by federal regulators, who routinely examine how banks collect, use, and retain data and enforce robust safeguards. By contrast, many nonbank providers holding comparable data are not subject to equivalent security standards or ongoing supervision, leaving critical gaps in protection.

GLBA Should Preempt Related State Laws

A key principle for any legislation in this area must be a national, uniform, financial privacy and information security standard with strong, clear federal preemption. Today, comprehensive state privacy laws are typically drafted for a broad universe of entities, some of which are in the business of monetizing data. Almost no other sector has the same responsibilities as banks in terms of using data to manage fraud and credit risk or that is subject to the same degree of prudential supervision from federal regulators.

Recognizing the distinct role of financial institutions, legislatures in most states have chosen to exempt GLBA-regulated entities at the entity level, with California an exception having exempted at the data level. Where state laws do reach into financial services, they can unintentionally interfere with core banking activities that can harm consumers, or create duplicative and conflicting obligations layered on top of the existing federal regime. Any modernized GLBA should provide a single, preemptive national standard for the privacy and processing of personal information by financial institutions, displacing banking-specific state laws in this space.

Privacy regulation for financial institutions should continue to be done on a sector-specific basis. Relatedly, any future comprehensive federal privacy law should recognize the distinct status of federally supervised financial institutions subject to GLBA and exempt them from overlapping requirements designed for very different business models. Applying multiple, inconsistent federal privacy regimes to banks would not improve consumer protection; it would increase complexity and legal risk, and could undermine effective fraud, anti-money laundering, and safety-and-soundness practices.

Enforcement

We strongly believe that enforcement of GLBA and any related privacy obligations for banks should remain with the appropriate federal regulators, not private litigants. Banking organizations are uniquely subject to consolidated supervision. Prudential and functional regulators already have powerful tools to drive better practices through examinations, guidance, and targeted enforcement. Introducing a private right of action in this space would encourage opportunistic litigation, create pressure for banks of all sizes to settle even where institutions are complying with the law, and divert resources away from investments in security and innovation, without meaningfully improving outcomes for consumers who are already protected by active regulatory oversight.

New Consumer Rights

To the extent Congress looks to incorporate concepts from state privacy laws, we urge a principles-based approach that respects the specific risk profile and legal obligations of financial institutions. Any new limits on collection, use, or retention should allow banks to gather and use information as relevant or necessary to provide requested products and services and for clearly disclosed purposes.

Data minimization and similar concepts must be implemented in a way that does not inadvertently curtail essential internal uses—such as fraud detection, cybersecurity, risk management, and the development of alternative underwriting models that can expand access to credit for underserved communities. Data elements like IP addresses or other information used in fraud consortiums can be pivotal in stopping scams before consumers are harmed; a rigid standard could make it harder, not easier, to protect customers.

If Congress is considering expanded individual rights such as access, correction, or deletion, it is vital that those rights be carefully tailored to the realities of banking. Deletion and similar rights must be reconciled with existing obligations, as well as with the need to preserve evidence of suspicious or criminal activity. GLBA's existing exemptions—for using data in connection with requested products and services, security and fraud prevention, risk control, and compliance with law—provide a useful model for any new rights in the financial sector.

Simpler, Clearer Privacy Notices

GLBA works well because of its clarity. But there is also room, in our view, to further modernize and streamline GLBA's notice requirements without changing the underlying balance of rights and obligations. Consumers expect a single, clear privacy notice that is easy to find and understand, not a stack of overlapping, state-specific documents. GLBA could be updated to better accommodate the use of a unified, plain-language notice—often made available online—that explains how data is collected, used, and safeguarded.

GLBA Should Remain Technology-Neutral

Finally, GLBA should remain focused on privacy and not be repurposed as a vehicle to regulate, for example, automated decision-making (ADM) or artificial intelligence (AI), in banking. One of GLBA's strengths is its technology-agnostic and principles-based approach, which allows banks and regulators to adapt to rapid changes without constantly rewriting the statute. If additional guardrails for AI or ADM become necessary, they can and should be addressed through tailored guidance, rather than by embedding technology-specific mandates into GLBA. There is also the risk that any prescriptive requirements could quickly become outdated, as well.

Conclusion

In closing, we believe GLBA has provided a durable, sector-specific federal privacy framework for more than a quarter century, underpinned by intensive prudential supervision for banks. If Congress decides to legislate in this space, we support targeted, carefully calibrated improvements paired with strong federal preemption, prudential regulator-based enforcement, and acknowledgement for the unique role that financial institutions play in protecting consumers and the financial system. We urge that any amendments do not disrupt existing practices that are necessary to fight fraud, money laundering, and terrorist financing. We stand ready to work with the Committee as you consider how best to preserve robust privacy protections for financial institutions while supporting innovation and helping them to meet the needs of their customers.

Thank you for your attention, and I look forward to your questions.