House Subcommittee Considers Modernizing Financial Services Under a National Privacy Framework

Laura Riposo VanDruff, Andrea deLorimier

June 6, 2025

On Thursday, the U.S. House Committee on Financial Services Subcommittee on Financial Institutions held a hearing entitled, “Framework for the Future: Reviewing Data Privacy in Today’s Financial System.” Hearing testimony explored whether there is need for a federal privacy statute and how the financial services industry, which is already regulated by the Gramm-Leach-Bliley Act ("GLBA") and other sector-specific statutes, would fit into such a standard.

Witnesses included Scott Talbott (Executive Vice President, Electronic Transactions Association), Andrew Morris (Director of Innovation and Technology, America’s Credit Unions), Rebecca Kuehn (Partner, Hudson Cook), Jennifer Huddleston (Fellow in Technology Policy, Cato Institute), and Zoë Strickland (Senior Fellow, Future of Privacy Forum).

We describe key themes from the hearing below.

- ***The patchwork of privacy laws in the U.S. is burdensome for financial services firms:*** Witnesses agreed that the U.S.’s patchwork approach to privacy has burdened the financial services industry, particularly its small to midsize players. For example, Ms. Huddleston noted that even though certain state privacy laws contain carveouts for data already regulated by the Gramm-Leach-Bliley Act or Fair Credit Reporting Act (“FCRA”), state privacy laws still affect and “create potential conflicts for” the financial services sector because they have different definitions of sensitive data or require specific steps in responding to consumer requests. According to various witnesses, this inconsistent patchwork harms consumers and stifles competition, as financial services firms are forced to allocate resources to compliance efforts instead of focusing on innovation. Moreover, some speakers, such as Mr. Talbott and Subcommittee Chair Andy Barr (R-KY), explained that the patchwork framework allows some states (i.e., California) to set a de facto national standard for privacy.

- ***Congress should create a national privacy standard:*** In light of the burdens posed by the patchwork framework, Mr. Talbott and Mr. Morris affirmatively voiced their support for a national, comprehensive privacy statute. They explained that a national framework would reduce compliance costs for financial services firms that currently devote substantial resources to state privacy law compliance. Representative Mike Flood (R-NE), during his questioning, expressed that while he supports states’ rights in almost every regard, a national privacy standard is the “one place” where he believes a federal framework is needed. Witnesses’ testimony also examined specific contours of a potential federal framework, including:

- No private right of action: Speakers uniformly agreed that a federal privacy statute should not include a private right of action or that any such right should be limited. For example, Chair Barr explained that a private right of action may incentivize plaintiffs' firms to file "frivolous" lawsuits against small or midsize players in the financial services industry that are less likely to be able to bear litigation costs. When asked by Chair Barr whether a private right of action would be prudent, Ms. Kuehn explained that financial regulators already have the tools at their disposal to protect consumers' financial data and that a private right of action is not needed. Ms. Huddleston pointed to Illinois' Biometric Information Privacy Act as an example of a statute with a privacy right of action that has led to adverse results, such as deterring innovation in already risk-adverse industries.

- Opt-out framework: Witnesses also agreed that any national privacy standard should align with GLBA's opt-out framework, at least as applied to financial services firms. As Representative Flood and Representative Roger Williams (R-TX) explained, financial services firms need to be able to provide consumers' personal information to process transactions, maintain accounts, and report to credit bureaus.

- Preemption: Chair Barr began the hearing by noting that there should be "clear, consistent, preemptive rules for financial institutions." In line with that theme, witnesses explained that any national privacy standard should preempt state laws. Similarly, with respect to GLBA, Representative William Timmons (R-SC) noted that the statute acts only as a floor for preemption, and that states are free to set different, higher standards. Ms. Kuehn echoed this theme, suggesting that if the Subcommittee were to reexamine the GLBA, it should reconsider whether GLBA should more broadly preempt state law.

- ***GLBA should continue to govern financial services firms:*** Witnesses largely agreed that the GLBA holds financial services firms to a high level of data privacy and security, and that it has, over the past two decades, successfully evolved along with the industry. As a result, witnesses expressed that the GLBA and other already-existing laws (such as the FCRA) should continue to govern financial services firms because they are tailored to the unique needs of the financial services industry. For example, Mr. Morris explained that any new federal privacy framework should offer an entity-level exemption for financial institutions already subject to the GLBA. Similarly, Mr. Talbott expressed that while a national privacy standard should be sector-agnostic, financial firms should continue to be governed by GLBA given the complexities of the industry.

- ***GLBA should retain ability to fight fraud:*** Ms. Kuehn explained that the under GLBA, certain exceptions permit firms to share consumer data without offering an opt-out option, such as when the data is used for fraud prevention. Ms. Keuhn continued that the CFPB's recently rescinded data broker rule could have jeopardized the ability of companies to use GLBA information for fraud prevention, and conflates the necessary actions of financial institutions with the actions of fraudulent bad actors. She therefore urged (as did Mr. Talbott) that when considering a new data privacy standard, the subcommittee should allow financial firms to continue to use data for fraud prevention.

The hearing highlighted that both lawmakers and industry participants alike see the need for a consistent framework to protect consumers' data and foster innovation and competition in the financial sector. The conversation is far from over, but the hearing marked an important step toward modernizing financial privacy for the digital age.