Testimony of Scott Talbott
Executive Vice President
Electronic Transactions Association

Financial Institutions Subcommittee of the House Financial Services Committee

Hearing on the Framework for the Future: Reviewing Data Privacy in Today's Financial System

June 5, 2025

Chairman Barr, Ranking Member Foster, and Members of the Subcommittee:

Thank you for the opportunity to testify on the important issue of data privacy in the financial system. I am Scott Talbott, and I serve as Executive Vice President at the Electronic Transactions Association (ETA). ETA is the leading trade association representing the entire electronic payments industry. Our more than 300 member companies facilitate safe, efficient, and innovative digital transactions in every state and across global markets, amounting to over $52 trillion globally. ETA members include payment processors, fintech firms, banks, hardware providers, and software platforms that form the backbone of the modern financial ecosystem.

ETA believes Congress should enact a single, uniform, comprehensive federal data privacy and data protection framework that protects consumers, supports innovation and operational agility, and ensures consistent national standards for the financial system.

Every day, our industry safely and securely helps power the American economy—whether enabling a small business to process its first digital transaction or facilitating contactless payments that enable consumers to make everyday purchases and to send money to each other. In every transaction, there is a shared expectation: that personal and financial data will be kept secure and handled responsibly.

Consumers rightly expect strong privacy protections and data security for their personal information and their money, and ETA fully supports the creation of comprehensive, uniform, federal data privacy legislation that upholds those expectations. But a federal data privacy framework must be thoughtful, workable, and grounded in how the financial system actually functions. It should provide consumers with the right to access, correct, and delete their information. It must balance strong consumer protections with the operational realities of protecting against fraud, enabling innovation, and supporting compliance. And it must preempt the growing patchwork of state laws that threaten to fragment the privacy landscape in ways that harm consumers and businesses alike.

The need for federal preemption is not theoretical. It is essential. As the University of Chicago Law Review noted in a 2020 article, "[a] fragmented legal regime can lead to inconsistent consumer outcomes, duplicative compliance costs, and reduced innovation in data-driven markets" (Richards & Hartzog, 2020). Privacy frameworks should provide clarity, not complexity. Consumers deserve consistent rights, and businesses deserve consistent rules, regardless of geography.

Today, two dozen states have enacted varying data privacy laws, with varying definitions, requirements, and enforcement regimes. This legal fragmentation creates extraordinary compliance burdens, especially for small and mid-sized companies that lack the resources of large multinationals.[1] A study by PwC found that over 50% of companies surveyed had to reengineer internal processes to meet divergent state privacy laws, with associated costs exceeding $1 million annually in many cases (PwC US, "Consumer Intelligence Series: Protect.me," 2022). Another study[2] found that state privacy laws could impose costs of between $98 billion and $112 billion annually. Over a 10-year period, these out-of-state costs would exceed $1 trillion. Of these costs, small businesses would bear $20–23 billion of this out-of-state burden annually.

The payments industry is not alone in calling for a federal solution. In a widely cited paper published in the Harvard Journal of Law & Technology, legal scholar Omer Tene observed: "The absence of a unified U.S. federal privacy regime has created both legal uncertainty and competitive disadvantages for American firms" (Tene, 2018). Moreover, organizations from the National Governors Association to leading consumer protection organizations like the Center for Democracy and Technology, Electronic Privacy Information Center, and Consumer Action, have supported legislation that harmonizes privacy rights and responsibilities under a federal umbrella.

A federal standard must also allow for the use of data to protect against fraud in order to protect consumers. The permissible use of data for fraud protection is essential to the safe operation of financial systems. ETA members use behavioral analytics, device recognition, biometric verification, and real-time pattern recognition to detect and mitigate identity theft, account takeovers, and fraudulent transactions. These systems rely on the responsible and secure use of consumer data.

For example, when a transaction originating in New York is suddenly attempted from Eastern Europe, fraud detection protocols may flag the discrepancy and seek to verify the transaction. We have all received notifications from our bank asking to verify a transaction. These systems—built over decades—are essential to the trust that underpins our financial system. That trust, and

---

[1] At the end of the document: ETA chart with examples of where state privacy laws conflict with each other.

[2] **50-State Patchwork of Privacy Laws Could Cost $1 Trillion More Than a Single Federal Law, New ITIF Report Finds (Jan 2022)**

those protections, would be weakened if well-intentioned privacy laws unintentionally restricted fraud mitigation efforts.

The European Union's General Data Protection Regulation (GDPR) acknowledges this balance. Article 6 of the GDPR expressly permits the processing of personal data without consent when "necessary for the purposes of the legitimate interests pursued by the controller" including fraud protection. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) similarly permits the collection and use of data for the purpose of detecting and mitigating fraud, without consumer consent.

Our view on this topic is straightforward: any U.S. federal privacy law should follow suit by embedding protections for the responsible use of data to detect, mitigate, and respond to fraudulent or suspicious activity. The Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), and Bank Secrecy Act all provide for these uses under existing law. *The Financial Data Privacy Act*, introduced last Congress by former House Financial Services Committee Chairman McHenry, built on this legacy by incorporating strong privacy rights while explicitly preserving fraud protection capabilities. That approach deserves to be the starting point for further legislative action.

The Financial Data Privacy Act was also notable for what it did not include: a private right of action. Private rights of action often result in class action litigation that does little to protect consumers while imposing significant costs on businesses. According to research by the American Tort Reform Association, the state with broad private rights of action for privacy violations have seen an uptick in lawsuits filed by plaintiffs' firms seeking large settlements, often with limited consumer benefit (ATRA Report, 2021).

Instead, enforcement should continue to reside with the appropriate expert federal regulators—such as the federal banking regulators and the Federal Trade Commission—that understand both the complexity of the data systems and the need for measured responses. Regulators have the expertise, experience, and tools to investigate, remedy, and monitor violations without stifling innovation or overwhelming courts.

Moreover, implementation timelines must be realistic. When California began enforcing the California Consumer Privacy Act (CCPA) during the height of the COVID-19 pandemic, businesses across the country faced significant uncertainty. With final rules issued just months before enforcement began, companies struggled to adjust compliance regimes amid workforce disruptions and supply chain issues. ETA joined a coalition requesting delayed enforcement not to avoid compliance—but to allow companies the time to implement it. Congress should avoid similar missteps in future legislation by ensuring clear, early guidance and extended implementation periods.

ETA and our members fully support strong data privacy rules. What we need are smart, coordinated, and enforceable regulations that protect consumers, enable innovation, and reflect how data powers the financial system. We are already subject to numerous privacy law and data protection laws and standards—including the GLBA Safeguards Rule, Fair Credit

Reporting Act, CAN-SPAM and Telephone Consumer Protection Act, PCI-DSS, and state cybersecurity regulations. Many of our members invest millions annually in data security, employee training, and third-party audits. We want accountability—but under one clear, national framework.

The payments industry constantly develops and deploys new products and services. Two developments in the marketplace are Open Banking and Artificial Intelligence. With Open Banking, financial information is, at the direction of the account holder, shared between banks, data aggregators, also called third-party providers. While most, if not all, of these entities are currently subject to GLBA's privacy and data security provisions (as banks or service providers) or indirectly through a relationship with a bank, policy makers should consider applying privacy laws to entities involved in Open Banking.

On Artificial Intelligence (AI) and other emerging technologies, policymakers should avoid regulating in the moment and instead should look for any gaps in existing laws and study any emerging risks that AI may create. Further, the payments industry is heavily regulated at the federal and state levels, and the long-standing use of rules-based AI by the industry is already subject to a number of laws and regulations, including fair lending laws. Any change in privacy law should consider existing laws and regulations and avoid stifling emerging technology.

Finally, any federal legislation should be technology-neutral. It should apply consistently across platforms and providers, whether the transaction happens on a mobile wallet, through a peer-to-peer app, or at a traditional bank branch. Financial privacy and data security should not depend on whether a consumer uses a fintech app or a debit card. Consistency is fairness.

ETA stands ready to assist Congress in developing and refining legislation that meets these standards. Specifically, we urge Congress to:

- Enact a comprehensive federal privacy and data security law that preempts state laws;
- Provide consumers with the ability to access, correct, and delete their data;
- Preserve the use of data for fraud protection and compliance;
- Assign enforcement to federal regulators;
- Provide clear, realistic implementation compliance timelines and guidance;
- Update definitions to focus on identified or identifiable individuals; and
- Establish technology- and sector- neutral standards.

Thank you again for the opportunity testify today. We welcome the opportunity to work with this Subcommittee to develop sound data privacy legislation that protects consumers and strengthens our digital economy.

Examples of Conflicting State Privacy Law Provisions

	Typical Approach	Conflicting State Approach
Applicability: B2B and employee	State privacy laws do not apply to individuals acting in commercial context, i.e., "B2B data" and employee data. *See all other state privacy laws.*	**California** applies to B2B data and employee data. Cal. Civ. Code § 1798.140(v)(1).
Scope of "Sensitive Data"	Sensitive data typically includes "personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status." *See, e.g.*, Va. Code § 59.1-575 "Sensitive data".	**Connecticut** and **Oregon** include individual's "status as a victim of crime" as sensitive data. Conn. Gen. Stat. § 42-515(38)(E); Or. Rev. Stat. § 646A.570(18)(a)(A).
		Maryland and **Oregon** also include data revealing "national origin." Md. Code, Com. Law § 14-4601(GG)(1)(vii); Or. Rev. Stat. § 646A.570(18)(a)(A).
		California additionally includes data revealing "philosophical beliefs" and "union membership," among a host of other data types, as sensitive data. Cal. Civ. Code § 1798.140(ae).
Data Minimization	Data collection and processing typically must be limited to what is adequate, relevant, and reasonably necessary to *the disclosed processing purpose*. *See, e.g.*, Va. Code § 59.1-578(A)(1).	**Maryland** requires controllers to limit data collection to what is reasonably necessary and proportionate *to provide or maintain a specific product or service requested by the consumer to whom the data pertains*. Md. Code, Com. Law § 14-4607(B)(1).
		California applies data minimization requirements additionally to data use, retention, and sharing. Cal. Civ. Code § 1798.100(c).
Consumer Rights Request Mechanisms	Many states allow the controller to determine "one or more secure reliable means" for consumers to exercise consumer rights. *See, e.g.*, Va. Code § 59.1-578(E).	Other states such as **California**, **Florida**, **Nebraska**, and **Texas** require that there be a method through the controller's website if the controller maintains a website. *See, e.g.*, Cal. Civ. Code § 1798.130(a)(1)(B); Fla. Stat. § 501.709(3); Neb. Rev. Stat. § 87-1111(3); Tex. Bus. & Com. Code § 541.055(c).
Responsibilities over Sensitive Data	Processing, including sale, of sensitive data is permitted only with opt-in consent from consumers. *See, e.g.*, Va. Code § 59.1-578(A)(5).	**Maryland** prohibits collecting, processing, or sharing sensitive data, even with consent, unless it is "strictly" necessary to provide or maintain a specific product or service requested by the consumer; sale is entirely prohibited. Md. Code, Com. Law § 14-4607(A).
Disclosure of Categories of Recipients of Data	States often allow consumers to request and obtain the *categories* of third parties to whom the controller shares personal information. *See, e.g.*, Cal. Civ. Code § 1798.115(a)(2). If no right to request such categories, then other states require controllers to disclose the categories of third parties on their privacy notice.	**Minnesota** allows consumers to request and obtain a list of *specific* third parties to whom the controller has disclosed personal information of that consumer. Minn. Stat.§ 325O.05(h).

	See, e.g., Va. Code § 59.1-578(C)(5).	