Testimony of Steven Boms

Executive Director

Financial Data and Technology Association

before the

Committee on Financial Services

United States House of Representatives

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

March 17, 2026

Introduction

Chairman Hill, Ranking Member Waters and members of the committee, thank you for the opportunity to testify today. My name is Steve Boms, and I am the Executive Director of the Financial Data and Technology Association ("FDATA").

FDATA is a leading trade association advocating for customer-permissioned access to financial data. Our members encompass a diverse ecosystem of financial technology ("fintech") companies, open banking platforms, and financial services companies that empower consumers and small businesses to leverage their own financial data to make informed decisions, access credit, manage their budgets, and improve their overall financial well-being. Across the country, FDATA members help more than 100 million American consumers and small businesses to more holistically manage and improve their finances in a competitive, heavily regulated ecosystem.

Before delving into the specific contours of any potential changes to existing federal data privacy legislation, it is essential to first contextualize the transformative impact that fintech has had for the way in which Americans interact with the financial sector. The rapid growth of the fintech sector has catalyzed an unprecedented era of innovation, injecting vital competition into the financial services marketplace, driving down costs to consumers and small businesses, and facilitating the more efficient delivery of critical financial services. This innovation directly benefits everyday Americans. Consumers use automated round-up apps to build high-yield savings by investing their spare change from everyday purchases like coffee or groceries. Real-time fraud notifications allow individuals to verify or block suspicious transactions at the point of sale, preventing unauthorized charges before they are even processed. Subscription management dashboards let users identify and cancel unwanted recurring fees with a single click, while investment platforms provide access to wealth-building tools that historically have only been available to high-net-worth Americans.

For small business owners, alternative underwriting platforms can help secure working capital based on their actual sales history and cash flow rather than relying solely on traditional credit scores. Mobile point-of-sale systems enable entrepreneurs to accept contactless payments anywhere using only a smartphone, significantly lowering the barrier to entry for new vendors. Integrated accounting software automatically syncs bank transaction data with digital ledgers to eliminate manual data entry, and invoice factoring platforms provide freelancers with immediate payment on outstanding work to keep their operations running smoothly.

The centerpiece of this ecosystem is trust. Third-party fintech tools inherently prioritize data privacy and security, not merely as a matter of regulatory compliance, but as the foundational imperative required to operate and maintain consumers' and small businesses' confidence. FDATA and our members strongly believe that consumers and small business owners should have full control over their financial data, including the right to share it with third parties free of charge, the right to withdraw their consent to have their data shared, and the right to understand exactly what data is being accessed for what purpose and by whom. This so-called "open banking" framework should, in our view, serve as the lodestar of any reconsideration of federal financial data privacy laws. Americans cannot be guaranteed data privacy if they cannot fully control their own financial data.

The Applicability of GLBA to Open Banking

A common misconception in the policy debate is that fintech companies and open banking platforms operate in a regulatory vacuum regarding data privacy. This is simply not the case. The Gramm-Leach-Bliley Act ("GLBA") already unequivocally applies to the data, the entities, and the data flows that constitute the open banking ecosystem and has done so since consumers and small businesses first began sharing elements of their financial data with fintech platforms more than two decades ago. The GLBA clearly and strictly governs the customer-permissioned financial data flows that open banking platforms and their fintech customers either enable or rely on to provide their product, service, or tool. This comprehensive regulatory coverage is established and enforced through three distinct mechanisms under the Act and its implementing regulations.

The "Significantly Engaged" Test

The GLBA and its implementing regulations, specifically the Financial Privacy Rule[1] and the Safeguards Rule,[2] apply to any entity "significantly engaged" in activities that are financial in nature or incidental to such activities. The Federal Trade Commission ("FTC") determines "significant engagement" based on the frequency and formality of the activity. An entity is considered significantly engaged if it performs financial activities as a regular and usual part of its business. For customer-permissioned open banking platforms, the core of their business model is the daily, high-volume transfer and processing of financial data. This is not an occasional or ancillary task; it is the primary service, meeting the threshold for significant engagement by default.

The 2021 "Finders" Rule

The FTC in 2021 expanded the application of its definition of a "financial institution" under the GLBA. Under the amended language, the definition of a "financial institution" includes any entity "acting as a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate…".[3] Many customer-permissioned open banking platforms facilitate these types of connections, effectively making them a "financial institution" for the purposes of the GLBA and placing them under the direct oversight of the FTC for GLBA compliance.

The Service Provider Provision

The relationship between a traditional financial institution, such as a bank, and a fintech or open banking platform is also governed by the GLBA Service Provider provision. Under 16 CFR § 314 and parallel banking agency guidelines, a financial institution is required by law to both exercise due diligence and vet the security and privacy practices of any third-party service provider before granting access to Nonpublic Personal Information ("NPI") and to mandate by contract that the third-party service provider implements and maintains administrative, technical, and physical data safeguards.

---

[1] *See* 16 CFR Part 313.

[2] *See* 16 CFR Part 314.

[3] *See* 16 CFR 314.2(h)(2)(xiii).

In practice, this means that every major open banking platform in the United States operates under a lattice of dozens, hundreds, or thousands of individual bilateral agreements, both with financial institutions that enable their customers to share data via application programming interfaces ("APIs") and with their third-party customers. Each agreement contractually mandates GLBA-level security and privacy features, with failure to comply constituting not just a breach of contract; it subjects the platform and its fintech customers to being cut off from the financial ecosystem entirely.

The net effect of these provisions of the GLBA and its implementing regulations has been to clarify that open banking platforms and the fintech tools they serve are all required to comply, today, with the relevant provisions of the Act, including the Safeguards Rule and the Financial Data Privacy Rule.

Third-Party Security and Privacy Obligations in Practice

Operating under the GLBA umbrella means that open banking platforms are already subject to rigorous, distinct, and highly prescriptive requirements for both their customers' data security and data privacy. Covered entities are legally required under the Safeguards Rule to develop, implement, and maintain robust, written information security programs ("WISPs") tailored to their size and complexity. They must designate at least one qualified executive directly responsible for the oversight, implementation, and continuous auditing of the company's WISP. They are required to utilize mandatory, state-of-the-art encryption protocols for data both in transit and at rest. They must continuously subject their systems to monitoring and rigorous penetration testing. And formal incident response and breach notification programs are mandated by law for any data breach event affecting 500 or more consumers.

Of course, a core element of data security is ensuring that customer data is only accessed with their informed consent and only for the purpose for which that consent has been granted. On this score, the GLBA requires transparency at the point of interaction. Accordingly, consumers and small businesses in the open banking context are presented with a clear, conspicuous privacy notice at the exact moment they connect their data through an open banking platform.

Pursuant to the GLBA, other statutory and regulatory requirements, and contractual obligations, open banking-enabled tools, products, and services operate on the principle of necessity. To the extent NPI is collected, robust data minimization programs ensure that the data accessed is strictly limited to what the customer has explicitly consented to and is necessary to effectuate the specific use case they have requested by the consumer. Moreover, the customer is provided the operational ability to revoke their consent and opt out of sharing their data at any time.

This robust security and privacy perimeter does not evaporate once data passes through an open banking platform. Just as stringent requirements flow down from banks to intermediaries, similar contractual obligations flow down to any subsequent third-party applications accessing and utilizing that data. The industry also proactively manages this risk. For instance, the Financial Data Exchange—the leading non-profit standard-setting organization for open banking—maintains a dedicated working group specifically focused on downstream data recipient risk management. This

ensures that privacy obligations, security audits, and compliance checks are rigorously enforced throughout the entire data lifecycle.

Open Banking Platforms Are Not Data Brokers

As the committee considers amendments to the GLBA, it is absolutely vital to draw a sharp legal and operational distinction between customer-permissioned open banking platforms and "data brokers." This distinction hinges on affirmative, explicit customer consent.

FDATA members access, route, and utilize data strictly because the customer has provided affirmative, informed permission to do so to receive a specific service, such as verifying income for a mortgage or connecting a bank account to a budgeting application. The consumer or small business is the active driver of the transaction. Conversely, "data brokers" acquire and sell end user data via secondary means, public records, and opaque tracking mechanisms, typically without the customer's direct involvement, knowledge, or consent.

In other policy contexts stakeholders representing large financial institutions have advocated for prescriptive secondary data limitations that would broadly target both customer-permissioned open banking platforms and "data brokers." FDATA strongly opposes conflating the two. Open banking platforms are already strictly bound under the GLBA and contractual terms by the consumer's or small businesses' explicit consent and the rigid data minimization requirements of their requested use case. Applying "data broker" regulations to customer-permissioned open banking intermediaries would negatively impact competition and consumer choice.

As previously discussed, the GLBA already obligates open banking platforms and, by extension, their fintech customers, to only access and utilize the NPI that is required to effectuate the specific use case they have requested and consented to. Introducing additional limitations on financial data access in excess of these existing obligations would risk hampering third parties' ability to enhance existing products and services and design new offerings; to protect their systems and customers from all manner of security threats; to alert consumers to more affordable or better-suited products or services; and from facilitating academic and policy research that is relied upon to inform monetary and fiscal decision making.

Ultimately, informed customer consent should continue to underpin Congress's approach to financial data privacy via the GLBA. That principle has been the backbone of the open banking marketplace that has for the last two decades enabled more than 100 million consumers and small businesses to access more affordable credit, to save more, to more easily file their taxes, to send and receive payments, and to better manage their finances.

Additional Policy Considerations

As Congress debates the overarching architecture of national data privacy, FDATA would respectfully urge the committee to carefully consider the following perspectives:

Data Portability

As it considers amendments to the Gramm-Leach-Bliley Act ("GLBA"), Congress take care not to undermine consumers' and small businesses' rights to data portability. Revisions to the Act that impose new requirements related to data minimization or that would require specific disclosures in instances in which a customer shares access to their data in certain circumstances could, unless carefully calibrated, inadvertently impede the data portability rights that consumers and small businesses have relied upon to manage and improve their finances with the support of third-party tools for more than two decades.

Moreover, because of the significant interrelationship between statutes governing data privacy and customer-permissioned data portability, Congress must be careful to avoid creating two incongruous federal financial data regimes. FDATA therefore urges the committee to ensure any legislative efforts by Congress to update federal data privacy laws harmonize with other statutes.

The Benefits of a National Financial Data Privacy Framework

FDATA supports a single, robust, and federally preemptive data privacy regime. The alternative—a fragmented, 50-state regulatory patchwork—is exponentially more costly to manage, creates massive compliance hurdles that disproportionately harm small startup innovators and favors large incumbents, and results in a highly inequitable system where a consumer's or small business owner's fundamental privacy rights are dictated entirely by their zip code.

The current decentralized approach to data protection and privacy in the U.S. is also at odds with the singular frameworks that have been deployed in other jurisdictions. Over time, this juxtaposition could have implications for attracting global investment and talent. For example, the General Data Protection Regulation ("GDPR") was a successful effort by the European Union ("EU") to end the era when every EU member had its own privacy laws and privacy regulator. While the merits of the individual components of GDPR are certainly open to debate, the concept of a single, pan-European data privacy regime unquestionably has streamlined customer protection and compliance across the Atlantic. A similar story is playing out in the United Kingdom ("U.K."), where the Smart Data Accelerator focuses on national interoperability for open finance. By providing a seamless, unified environment, the U.K. aims to attract fintech capital that might otherwise be deterred by the complexity of the U.S. market.

Only Congress can provide the clear, unified rules of the road the digital economy requires.

Because data within it is already so heavily regulated under the GLBA, financial services represents one of the few marketplaces in which Congress can leverage a federal regime that already broadly applies and has served consumers well for nearly 30 years. Because the financial sector already operates under the rigorous, long-standing requirements of the GLBA and the Fair Credit Reporting Act ("FCRA"), it possesses the mature compliance infrastructure necessary to serve as the logical vanguard for a national data privacy standard. This phased approach would mirror the successful implementation of international models like Australia's Consumer Data Right, which intentionally prioritized the banking industry as its inaugural designated sector to refine privacy and data portability protocols before expanding them to the rest of the economy. By building upon these existing, tested frameworks, Congress can establish a high baseline for

consumer protection while minimizing the market friction typically associated with entirely new regulatory regimes.

Deletion and Termination
Consumers and small business owners should absolutely possess the right to affirmatively request that their data be deleted or that data sharing be terminated immediately. The sole exception to this rule must be narrowly tailored instances where a valid legal or regulatory order, such as anti-money laundering preservation requirements or law enforcement orders, mandates data retention. In promulgating any national data deletion right, Congress should also carefully consider other statutory obligations under which financial institutions, fintechs, and customer-permissioned data access platforms operate that may include data retention requirements, such as the FCRA.

Data Correction
In the open banking context, the obligation and legal liability to correct inaccurate data must remain squarely with the data provider and not the customer-permissioned open banking platform or the fintech that relies on that platform for its data access. Open banking platforms act as technological conduits; they securely transport data but do not, and cannot, alter the underlying source data. Furthermore, in cases involving lending and credit decisions, the FCRA already mandates a comprehensive, battle-tested data correction regime. Beyond the technical barriers, requiring intermediaries to undertake data correction responsibilities could result in situations in which both the data provider and the customer-permissioned open banking platform may generate redundant or conflicting consumer records. This misalignment would undermine data accuracy, confuse consumers, and impose unnecessary burdens on platforms, ultimately detracting from the intended clarity and efficacy of the FCRA framework.

Enforcement
Any federal data privacy legislation should maintain the GLBA's agency enforcement mechanisms. In other federal privacy laws, such as the FCRA, our members have seen how private rights of action have threatened businesses with ruinous litigation that conveys no discernable consumer benefit. By delegating enforcement to agencies rather than private litigants, Congress can ensure expert, uniform oversight of consumer privacy without harming innovation and competition.

Conclusion

On behalf of FDATA's member companies, thank you, Chairman Hill, Ranking Member Waters, and members of the committee, for the opportunity to testify today. Our members provide your constituents with important financial products, services, and tools on which they rely to manage their financial well-being. They make the financial marketplace more competitive, more innovative, and more convenient, and always prioritize protecting their customers' data privacy and security.

As the committee considers legislation to modernize financial data privacy, I strongly urge you to carefully consider the interrelationship between data privacy and the ability of a consumer or small business to elect to share elements of their financial data with third-party financial tools as an important consideration of any new federal privacy legislation.

Thank you again for the opportunity to testify. I look forward to answering your questions.