https://fdata.global/north-america/

August 28, 2025

The Honorable French Hill
Chairman
Committee on Financial Services
United States House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
United States House of Representatives
4340 O'Neill House Office Building
Washington, DC 20515

The Honorable Andy Barr
Chairman
Subcommittee on Financial Institutions
United States House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Bill Foster
Ranking Member
Subcommittee on Financial Institutions
United States House of Representatives
4340 O'Neill House Office Building
Washington, DC 20515

Submitted via electronic mail to fsc119@mail.house.gov

Dear Chairman Hill, Ranking Member Waters, Chairman Barr and Ranking Member Foster,

The Financial Data and Technology Association ("FDATA") appreciates the opportunity to provide comments in response to the House Financial Services Committee's and the Subcommittee on Financial Institutions' request for feedback on current federal consumer financial data privacy laws and potential legislative proposals to account for changes in the consumer financial services sector. As the financial services ecosystem continues to evolve alongside seismic technological advancements, a comprehensive federal data privacy regime that takes into account how personal data is collected, used, shared, and protected is paramount; however, it is also important that any financial data privacy framework implemented moving forward upholds the protections already established under the Gramm-Leach-Bliley Act ("GLBA") and existing regulations under both that statute and others with which many financial services providers already comply to protect consumer data.

About FDATA

FDATA and our member companies have for years been strong advocates for providing consumers, small business owners, investors, and other financial services marketplace end users with legally binding financial data rights. As we have seen in other jurisdictions around the world

that have granted their citizens legal rights and protections ensuring the ability to access and share their financial data, a customer-centric ecosystem in which the end user is in full control of their data leads to a more innovative, more competitive, and more transparent financial marketplace.

Our members' products, services, and tools underscore this reality. FDATA was founded in early 2018 by several financial technology firms whose technology-based products and services allow consumers and small and medium enterprises to improve their financial wellbeing. As the leading trade association advocating for consumer-permissioned access to financial data, FDATA members include firms with a variety of different business models. Collectively, our members provide more than 100 million American consumers and small business owners access to vital financial services and products, either on their own or through partnerships with supervised financial institutions. Regardless of their business model, every FDATA member's products or services share one fundamental and foundational requisite: the ability of a customer to actively permission access to some component of their own financial data that is held by another financial services provider.

Committee Questions on Title V, Subtitle A of the GLBA

1. ***Should we amend the Gramm-Leach-Bliley Act (GLBA) or consider a broader approach?***
   The GLBA has set the framework for how data privacy is governed in the financial services industry for decades. For financial technology companies who meet the definition of "financial institution" under the Act, the GLBA has set a high standard by prescribing important data privacy protections, including mandatory consumer disclosures around data sharing practices and the safeguarding of sensitive financial data.

   From a logistical perspective, the committee should be mindful that various states have incorporated GLBA by reference into their respective state privacy laws, either as part of their compliance requirements or as a preemptive or partially preemptive federal framework. Should the committee consider an approach other than amending the GLBA, the resulting complexity between state and federal financial data privacy requirements could undermine the intended result of this exercise, which is to streamline consumer financial data privacy and the associated compliance requirements for financial services providers across the country.

   For these reasons, FDATA recommends working within the contours of the GLBA rather than considering a broader approach.

2. ***Should we consider a preemptive federal GLBA standard or maintain the current GLBA federal floor approach?***
   A federal data privacy regime in the United States is critical for establishing clear and consistent standards for how personal information is collected, used, and secured. A federal data privacy regime is also essential to ensure uniform, effective, and future-ready protection of personal data, to streamline compliance and promote innovation in a manner that enables

smaller entities to scale, to promote clarity and consistency for businesses, and to position the United States as a global leader in data governance and interoperability.

From a consumer privacy rights perspective, a federal preemptive standard would ensure consistent protection of personal data irrespective of which state in which a consumer resides and should facilitate uniform financial data rights, including financial data access, correction, and deletion rights, among others.

3. ***If GLBA is made a preemptive federal standard, how should it address state laws that only provide for a data-level exemption from their general consumer data privacy laws?***
   As discussed above, a federally preemptive financial data privacy statute would create certainty for consumers and small businesses and would improve innovation and competition in the financial services system. To be maximally effective, the committee should consider a preemptive privacy framework in which there are broad entity level carve outs from state law for entities subject to GLBA. Conversely, a privacy framework that promotes data-level exemptions creates complexity and uncertainty regarding the scope of GLBA exemptions.

4. ***How should GLBA relate to other federal consumer data privacy laws, both a potential general data privacy law and current sector-specific laws?***
   FDATA urges the committee to view amendments to GLBA as a chapter of a broader preemptive data privacy statute.

5. ***How should we define "non-public personal information" within the context of privacy regulations?***
   The GLBA outlines protections for non-public personal information (NPI) including the Privacy Rule (16 CFR Part 313), which requires financial institutions to provide privacy notices and limit disclosure of NPI; and the Safeguards Rule (16 CFR Part 314), which notes that institutions may not disclose NPI to nonaffiliated third parties unless the consumer is given notice and opportunity to opt out or an exception applies. FDATA asserts that any amendment to the definition of NPI should be supplemented to reflect new technologies in the financial services ecosystem, including IP addresses, mobile device IDs, behavioral data, and authentication tokens. However, GLBA definitions are well understood within compliance systems and should not be changed materially unless there are clear gaps that lead to consumer harm, aggressively amending established definitions could disrupt consumer access.

   a. ***Does the term "personally identifiable financial information" in GLBA require modification?***
      The definition of "personally identifiable financial information" in the GLBA excludes "information that does not identify a consumer, such as aggregate information or *blind data that does not contain personal identifiers such as account numbers, names, or addresses.*" This information, also known as pseudonymized data, is not "non-public personal information" and thus is currently excluded from the GLBA

coverage. This approach is consistent with other global data privacy frameworks, including Europe's General Data Protection Regulation (GDPR), and allows pseudonymized data to be used to build new products, enhance existing tools, and perform research, among many other use cases. Failure to continue to exclude pseudonymized data from "personally identifiable financial information" risks the U.S. market falling behind on digital financial innovation with little to no commensurate additional consumer protection. Therefore, FDATA asserts that any redefining of this term must ensure that pseudonymized data continues to be excluded from the definition.

6. ***Do the definitions of "consumer" and "customer relationship" in GLBA require modification?***

   The definitions of consumer and customer relationship under GLBA are sufficiently broad as to cover the overwhelming majority of individual's relationships with financial services companies and thus FDATA is satisfied with the existing definitions.

7. ***Does the current definition of "financial institution" sufficiently cover entities that should be subject to GLBA Title V requirements, such as data aggregators?***

   The GLBA defines "financial institution" as any institution the business of which is engaging in financial activities as described in the Bank Holding Company Act of 1956. FDATA's aggregator member companies are covered under this definition of "financial institution" under the GLBA and adhere to the privacy and safeguards requirements outlined in the Act.

   As the committee reviews the definition of "financial institution" under GLBA, FDATA believes it is important to distinguish between traditional data aggregators, who only access data at the express consent of the consumer with their permission and are inarguably already covered under the statute, and entities that access and maintain consumer records in the absence of such affirmative consent, which may not be. A clear distinction between these two very different types of interactions with consumer data – one with the consumer's express consent and another in some instances without it – would better reflect the current realities of the consumer data access marketplace.

8. *Are there states that have developed effective privacy frameworks?*
   a. *Which specific elements from these state-level frameworks could potentially be adapted for federal implementation?*

9. ***Should we consider requiring consent to be obtained before collecting certain types of data, such as PIN Numbers and IP addresses?***

   FDATA stands by the notion that consent is the cornerstone to financial data access, and FDATA members rely on express consumer consent before accessing a consumer's sensitive financial data.

In so doing, it is important for the committee to also consider existing use cases, like fraud prevention, that rely on access to certain data elements to protect consumers from misuses of their data.[1] For example, the collection of an IP address, which is not on its own sensitive, may be used to fuel various use cases, including fraud prevention. The requirement to capture consent to collect this information would undermine the important use cases that foster consumer protection. In other words, consent for this type of non-sensitive data would create friction without consumer benefit and would inhibit beneficial consumer protection services.

10. ***Should we consider mandating the deletion of data for accounts that have been inactive for over a year, provided the customer is notified and no response is received?***

FDATA stands by the notion that consumers own, and determine who has access to, their data. Additionally, FDATA and our member companies agree, and follow the practice that data aggregators and third parties must delete consumer data when the consumer revokes access; the data is no longer necessary for the product or service; or when the relationship with the consumer ends. These requirements, among others, are meant to limit unnecessary data retention and reduce privacy and security risks.

However, FDATA views a disconnect between the data deletion or revocation standards and the reauthorization standards as outlined in the rule, which state that third parties must obtain authentication from consumers at least once every 12 months to maintain a connection and retain account data. This requirement interferes with well-established use cases including recurring payments, personal financial management tools, cash-flow underwriting, e-commerce payments, and others, for which consumers may have no need to authenticate annually but still rely on their data being accessible. For example, a 12-month data deletion mandate could force a consumer to reenter all of their financial information to fuel a tax preparation tool if they filed their taxes in March in one year and April the next. The same potential for consumer harm exists with regard to recurring payment use cases. An individual may set up a monthly pay-by-bank autodraft for their wireless bill and would be surprised on month 13 to find that it wasn't paid. Additionally, a 12-month reauthorization and data deletion mandate for open banking use cases also raises competition issues by putting open banking-enabled payments at a competitive disadvantage to traditional card payments, because merchants do not need to ask consumers to reauthorize their payment card information every 12 months. This could lead to further concentration in the payments sector.

[1] IP address data, for example, is frequently accessed when a user attempts to log in to an account as a fraud prevention measure. In instances in which an IP address suggests the log in attempt is emanating from a location different than the one a consumer typically logs in from, a provider may prompt a multi-factor authentication requirement.

11. ***Should we consider requiring consumers be provided with a list of entities receiving their data?***

    Under existing law, disclosures are already required by financial technology providers for transaction data in Regulation E and Regulation Z accounts. A similar approach under GLBA would ensure that banks would be required to provide similar disclosures to their consumers.

12. ***Should we consider changing the structure by which a financial institution is held liable if data it collects or holds is shared with a third-party, and that third-party is breached?***

    FDATA has long stood by the notion that the entity who imposes financial harm to a consumer is the entity responsible for making the consumer whole. However, given the process through which data is obtained and received, apportionment of liability can often be hard to pinpoint.

    In reality, the issue of liability has evolved into a red herring, away from its intended effort to ensure accountability and towards anticompetitive and inaccurate assumptions. In truth, Congress and the financial regulatory agencies have meaningfully addressed this complex issue through statute including the Truth in Lending Act, the Fair Credit Reporting Act, and the Electronic Funds Transfer Act, which financial regulatory have implemented through various regulations. Financial technology providers are also overseen by the prudential regulatory agencies, the CFPB, and the Financial Industry Regulatory Authority. Industry frameworks, including the National Automated Clearing House Association (NACHA) also address liability in the payments sector. In sum, there exists today a comprehensive, albeit somewhat fragmented, liability framework that protects consumers when their data is misused and provides that the entity responsible for a breach be liable for any consumer harm.

    Rather than assuming the liability framework in the financial sector must be completely reimagined, FDATA recommends the committee acknowledge the existing liability frameworks already established in the financial services ecosystem and identify gaps in current statute regulation, ultimately considering targeted amendments to existing law to address them.

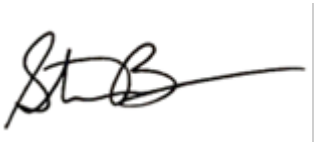
13. ***Should we consider changes to require or encourage financial institutions, third parties, and other holders of consumer financial data to minimize data collection to only collection that is needed to effectuate a consumer transaction and place limits on the time-period for data retention?***

    The Consumer Financial Protection Bureau's Section 1033 final rulemaking enforces financial data safety and security mandates on third parties by, among other requirements, requiring compliance with information security and data minimization standards. The underlying premise of the Bureau's final rulemaking is that consumers, not their banks, choose who to share their financial data with, how it will be accessed, and who will use it. The GLBA should recognize these important realities in statute, to ensure that banks are not permitted to enforce their views of data minimization, retention, or deletion standards on third parties.

This shift in oversight would create market confusion and an anticompetitive environment, undermining the important tenet that consumers should at all times be in full control of their financial data.

Thank you for the opportunity to provide comments to the committee on current federal consumer financial privacy laws and potential legislative proposals to address the changes in our consumer financial services sector. FDATA and our member companies stand ready to provide additional information or feedback as the committee considers next steps.

Sincerely,



Steven Boms
Executive Director