August 28, 2025

The Honorable French Hill
Chairman
House Committee on Financial Services

The Honorable Andy Barr
Chairman
Subcommittee on Financial Institutions

Via email: fsc119@mail.house.gov

Re: Request for Feedback on Current Federal Consumer Financial Data Privacy Law and Potential Legislative proposals

Dear Chairman Hill and Chairman Barr:

On behalf of SentiLink, we are pleased to submit the following comments in response to your request for comments related to "Current Federal Consumer Financial Data Privacy Law and Potential Legislative Proposals."

About SentiLink

SentiLink provides identity verification, fraud mitigation and risk management solutions to US-based financial institutions, telecommunication companies, government agencies and others. In the context of financial services, SentiLink's solutions ensure that applicants are who they claim to be, enabling institutions and individuals to transact confidently with one another by preventing identity fraud at the point that a consumer is applying for any type of financial account. SentiLink was also the first company in history to use the Social Security Administration's Electronic Consent Based SSN Verification service ("eCBSV") to validate account application data, as well as the first service provider to integrate with the U.S. Treasury Department's enhanced Treasury Check Verification Service ("TCVS") Application Programming Interface ("API").

Each day SentiLink helps over 3,000,000 consumers applying for financial products and services, and in doing so prevents approximately 60,000 cases of identity fraud daily. Underneath the surface of our solutions are statistical models continually trained and improved by three primary sources: First, data from external and highly vetted sources; second, our team of expert risk analysts who review and manually investigate cases to stay abreast of the leading edge of fraud tactics and criminal activity, feeding that knowledge into model updates; and third, data provided by our clients (referred to as "partners"). We do not collect or rely on demographic data and have a robust process in place for independently auditing our scoring models, including statistical assessments of impacts across demographic groups by a third-party economic analysis firm.

Our models deliver real-time fraud scores and signals via API to our partners to help ensure:

- Legitimate customers, including thin file and those new to credit, get onboarded quickly;
- Consumers are protected from identity crime;
- Fraud in the financial system is reduced; and
- Financial regulatory obligations are satisfied.

It is from this perspective that we offer the following feedback to select questions:

1. Should we amend the Gramm-Leach-Bliley Act (GLBA) or consider a broader approach?

GLBA's existing framework appropriately recognizes the uniquely sensitive nature of financial data and the need for robust consumer protections. By any measure, it is the gold standard of sector-specific privacy laws in the U.S.. That said, we applaud the Committee for undertaking an effort to modernize this critical but increasingly timeworn statute.

Not to be overlooked in any modernization is the current exemption at section 6802(e)(3). Under that exemption, a financial institution is not required to provide a notice or an opt-out opportunity if the disclosure of nonpublic personal information is to "protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability." We encourage the Committee to preserve and strengthen this exemption. As witnessed in a recent proposed rulemaking,[1] misguided policies risk undermining financial institutions' ability to prevent fraud by eroding the fraud prevention exemption and misapplying regulatory constraints to the very tools and data needed to protect consumers from identity fraud.

Regardless of whether Congress pursues a broader, omnibus approach or maintains a sector-specific structure, we urge the Committee to maintain the historical precedent that preserves beneficial use cases of consumer data -- such as identity verification and fraud prevention activities -- by exempting these activities and the data necessary to make them effective from general privacy law requirements.

2. Should we consider a preemptive federal GLBA standard or maintain the current GLBA federal floor approach?

[1] https://www.federalregister.gov/documents/2024/12/13/2024-28690/protecting-americans-from-harmful-data-broker-practices-regulation-v.

We strongly encourage the Committee to pursue a preemptive federal privacy standard. Identity fraud operates across state lines. As financial services increasingly transition to digital platforms and electronic payments, patchwork state regulations create compliance complexity and inconsistencies that can weaken fraud prevention effectiveness. A federal standard that maintains a robust exemption for identity verification and fraud prevention activities would ensure critical fraud prevention data sources and processes remain available nationwide.

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?

If Congress maintains a sector-based approach to privacy policy, the Committee should ensure that updates to GLBA provide financial institutions with field preemption from any requirements in state data-level-based laws that would undermine the ability of financial institutions to vigorously prevent identity fraud as contemplated (and protected) by the GLBA.

a. Should GLBA "financial institutions" be subject to entity-level or data-level exemptions from these laws?

If an entity is subject to and in compliance with a federal privacy regime, state privacy laws on the same matters should be preempted to avoid confusion, conflict, and any weakening of the federal policy in support of identity protection and fraud prevention.

In our experience providing identity verification and fraud prevention tools to financial institutions with consumers in every state, the policy tension between data- versus entity-level exemptions is not significant in practice. Therefore, we recommend a hybrid approach: As this Committee is well aware, financial institutions face unique regulatory obligations under BSA/AML laws that require specific data practices and uses. In the context of GLBA *and* a general privacy law, maintaining entity-level exemptions applicable to financial institutions and their fraud prevention service providers prevents regulatory conflicts between privacy laws and financial crime prevention requirements.

Within that entity-level structure is the question of what entities are covered, and here we recommend looking to the precedent in GLBA: While the overall statute is entity-based, GLBA coverage is determined instead by an evaluation of what the entity actually does. Specifically, GLBA's definition of "financial institution" is activity-based, and has evolved over time as the Federal Reserve and courts have provided additional interpretations that support a robust financial services marketplace. This adaptive definition has allowed the body of financial data privacy regulations established in the statute to expand in scope as the industry has changed. While data- versus entity-level considerations will be top-of-mind for many, the additional use of activity-based exemptions and categorizations as policy choices may allow for more regulatory flexibility in the future. This flexibility, in turn, will enable regulators to avoid unintended consequences, such as weakened identity theft prevention, that disserve both financial institutions and consumers.

5. How should we define "non-public personal information" within the context of privacy regulations?

The current GLBA framework, including the definition of "non-public personal information," is generally appropriate. Closely related to this definition are critical exemptions for beneficial use cases. We recommend the legislation include an appropriate definition for "*identity verification and fraud prevention activities*," which means the strategies, practices, data and systems that are acquired, built, trained, refined, and employed to detect, deter, and mitigate the misuse or misrepresentation of identities, and otherwise avert identity-related financial crime. Including such a definition will solidify and clarify the importance of this beneficial use case. At the same time, it will appropriately limit the extent to which such an exemption could be used to evade consumers' privacy rights by differentiating genuine fraud prevention use cases from other business activities.

Consolidated response to questions 9, 10 and 13:

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

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?

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?

Many identity verification and fraud detection solution providers to financial institutions rely on high-quality data inputs to build models that can determine with high accuracy whether someone is who they claim to be, are a victim of identity fraud, or are attempting to commit identity fraud themselves. As it relates to the many nuances of consumer data usage that are likely to be considered by this and other committees, we simply urge the following: It is imperative that beneficial use cases, including identity verification and fraud prevention activities, be exempt from restrictions or limitations that would inadvertently compromise their effectiveness. In the absence of such exemptions, the likelihood that well-intended policies result in negative consequences for consumers grows significantly.

Using two of the posed questions as examples:

- Requiring consent to obtain certain types of consumer data, such as IP addresses, is likely to hamper fraud prevention activities: A criminal attempting to commit identity theft is unlikely to grant consent to a financial institution knowing that such data may be used to detect their illicit activities. As a result, the financial institution and its fraud prevention service provider are deprived of a powerful fraud signal to detect the criminal activity. If Congress pursues consent-based requirements for certain types of data collection, such requirements should exempt identity verification and fraud prevention use cases and associated data.
- Some types of identity verification and fraud detection models gain their precision and accuracy by evaluating identities based on historical data. If identity verification and fraud detection solution providers are required to delete data upon a consumer's request -- something a smart identity criminal would likely take advantage of -- it would become materially harder to protect actual victims of identity fraud. The same logic applies to deletion based on a period of inactivity, as criminals actively seek out identities with inactive periods (such as older consumers and consumers residing outside the United States) as ripe targets for identity theft. Again, should Congress pursue data deletion requirements, such a provision should exempt identity verification and fraud detection activities and associated data.

Thank you for the opportunity to provide SentiLink's perspectives on these important questions. We look forward to working with you and your colleagues on the Committee as the legislative process moves forward.

Sincerely,

/s/
Jason Kratovil
Head of Policy and External Affairs

/s/
John Leitner
General Counsel (Product & Regulatory) and Head of Privacy