February 24, 2023

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

Dear Chairman McHenry:

The undersigned insurance trade associations support your efforts in introducing the Data Privacy Act of 2023 - legislation that will modernize the Gramm-Leach-Bliley Act (GLBA), a working data privacy framework for insurance consistent with consumer expectations. The insurance industry is proud of its longstanding role as a conscientious and responsible guardian of customers' personal information. Our industry has appropriately managed consumers' confidential medical and financial information for decades. Fittingly, insurers and producers (agents and brokers) have long been subject to comprehensive federal and state privacy laws and regulations. These requirements provide a complex, broad and rigorous regulatory framework that requires our industry to protect the privacy, use and security of consumers' personal information. These laws have reflected a critically important balance between consumers' legitimate privacy concerns and the proper use of personal information to the benefit of existing and prospective customers. We remain strongly committed to the proper use and protection of our customers' personal information.

In anticipation of the February 28th, 2023 markup of the Data Privacy Act of 2023, we respectfully request that the following changes be made to the text:

Notice requirements (Sec. 502(b)(1) / Discussion Draft Section 3, pg. 3) – To be consistent with requirements in other jurisdictions and to avoid operational challenges, we would recommend clarifying that providing the notice may be concurrent with collecting the information and that no opt out opportunity need be provided if collection and disclosure is done only for purposes within an exception. This could be addressed through the following edits:

> Section 502 (b)(1) Opt Out
> In general- A financial institution may not disclose collect nonpublic personal information from a consumer or disclose nonpublic personal information to a nonaffiliated third party unless – the consumer is given the opportunity, at or before the time that such information is initially collected or disclosed, to direct that such information not be collected or disclosed to such third party, or it falls within one of the exceptions.
>
> Section 502(e) Exceptions
> The general collection, ~~and~~ disclosure, and opt-out procedures provided in subsections (a) and (b) shall not prohibit or otherwise limit the collection or disclosure of nonpublic personal information—

Notification to nonaffiliates when sharing is terminated (Sec. 502(f) / Discussion Draft Section 3, pg. 7) - The bill (and existing GLBA language) allows consumers to opt out of sharing personal information unless an exception applies (such as sharing personal information with a third party to service the consumer's account or provide marketing services to the financial institution). The new additional requirement in Section 502(f) requires

financial institutions to, in situations where a consumer is permitted to opt out of sharing with nonaffiliated third parties, notify the third party that the sharing has been terminated and that the third party can no longer share the consumer's NPI that it already received. We would typically be able to rely on an opt out exception for most sharing of personal information with third parties, but to the extent there are opt outs that do not fall within the exception it could be burdensome to have to notify each third party that the opt out occurred. Notification to a third party where sharing is terminated as part of a relationship seems reasonable; however, this should be pursuant to an agreement and should be from the effective date and implementation time moving forward. Additionally, it should be clear that this does not include nonpublic information where an exception exists. These changes could be accomplished by at the end of Sec. 502(f)(1) by inserting "…*after a consumer exercises an opt out under subsection (b)*" and at the end of Sec. 502(f)(1)(b) inserting "…*except as provided for in subsection (e)*."

Data Retention (Sec. 503(d)(6) / Discussion Draft Section 4,pg. 11) - Data retention policies are incredibly complex and granular. Including data retention policies and specific periods of time in a privacy notice would make the notice considerably longer than it is now and likely unreadable for the average consumer., . It will result in significant work with little consumer benefit. If included in the notice content requirements, we suggest that the language be clarified to indicate that the retention disclosure should describe at a high level how retention periods are determined. This might be accomplished through section 503(d)(6) language similar to: "*the considerations used in the development of the data retention policies of the financial institution*."

Customer or Consumer Relationship (Sec. 509(11) / Discussion Draft Section 8, pg. 15) - We are concerned with the definition of Customer or Consumer Relationship because insurers have no ongoing business relations with a "Consumer." The impact of this definition to insurers would include, for example, the need to provide a privacy notice with every insurance premium quote or illustration. Especially in the context of independent agents assisting consumers shopping for coverage, this could significantly expand the number of notices consumers receive. We suggest that non-customer exemptions be expanded to include "in connection with an insurance quote or premium illustration."

Certain Inactive Accounts (Sec. 502A / Discussion Draft Sec. 9, pg. 19) - While it may make sense to not allow Data Aggregators to hold onto accounts and user data that are now dormant and inactive, it does not make sense for long-tail financial products like life insurance or long-term care, single premium products where they may not be any transaction for a very long period of time, or property-casualty products where there may later be claims for latent risks. Compliance with this provision would be very burdensome and costly, with little value to the consumer. Additionally, it also goes against the current trend (such as in the FAST Act) to limit situations in which financial institutions need to send annual privacy notices to their customers so long as certain conditions are met. Indeed, it may have the surprising impact of requiring more ongoing notices to be sent to former customers than to current customers. We suggest the provision be removed in its entirety. Alternatively, we suggest clarifying that when there is no obligation to delete information, there is no requirement to notify a customer (and allowing for a web posting and/or satisfying section 503(g) as alternatives to the recurring annual notice under (B)). Further, the exception in section 502A(b)(3) could be amended to state "*This subsection shall not require a financial institution to notify the consumer under subsection (b) or delete nonpublic personal information if*…..".

Format (Sec. 502A(2) / Discussion Draft Sec. 9, pg. 19) – The proposed "access to information" provisions of the bill call for a "structured, commonly used, machine-readable" format in which these disclosures would be required. These particular elements are unworkable for most insurance licensees (including small insurance agencies), impose costly new obligations, and do not significantly benefit insurance consumers. We suggest the

following language, based on and mirroring the text in the Section 503(b) privacy notice requirements- "*Disclosures described under paragraph (1) shall be in writing, or in electronic form, or other form as permitted by the regulations prescribed under section 504*."

Essential Workability: Scope, Exceptions, & Timing – Financial institutions differ between sectors. For insurers and producers, privacy requirements must allow not only for consumer protection but also for: (1) operational uniformity; (2) adequate time to implement new and revised requirements, and (3) exceptions necessary to conduct the business of insurance. For operational uniformity, the scope and preemption language are vital to the insurance industry. With this in mind the inclusion of the word "use" of nonpublic personal information is critical to include within section 507(1). We suggest the provision should read *"(1) the collection, use, or disclosure of personal information;…*". For implementation, the new requirements (and forthcoming regulations) must be *prospective* in nature and contemplate an effective date taking effect no sooner than 2 years after the date rules are finalized. The importance of taking this approach time and period within effective date language under section 510 cannot be overstated. Finally, exceptions are critically important to insurers – as well as to agents and brokers – being able to do business and serve customers across the country. We wanted to highlight necessary items beyond those mentioned above.

> In section 502(e)(1) , expanding (B) by adding wording at the end: "… *or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise preform or relate to a contract between the business and the consumer*."
>
> In section 502(e)(3), expanding (B) by adding at the end: "…*malicious, deceptive, or illegal activity, or to exercise or defend legal claims*."
>
> In section 502(e)(4) inserting "… *statistical agents, reinsurance, stop loss, or excess of loss insurance,*"
>
> In section 502(e)(8) inserting "*inquiry*" before "investigation" and adding "*or court order*" after "local authorities."
>
> In section 502A(b)(3)(A) adding "*The nonpublic personal information is necessary or may be used to: (a) help to ensure security and integrity to the extent the use of the consumer's nonpublic personal information is reasonably necessary and proportionate for those purposes, or (b) fulfill the terms of a written warranty or product recall conducted in accordance with applicable law*."

Again, a landmark privacy framework should continue to both protect nonpublic personal information and remain consistently workable for all financial institutions including insurers, agents, and brokers, to serve their customers and consumers. It relies on many details, including those relating preemption, scope, exceptions and timing.

Conclusion

We, the undersigned organizations, thank you for your leadership in sponsoring and marking up this bill. We look forward to working with you and your staff to advance this legislation.

Please do not hesitate to contact any of the organizations below with questions.

Sincerely,

American Council of Life Insurers
American Property Casualty Insurance Association
Council of Insurance Agents and Brokers
Independent Insurance Agents and Brokers of America
Insured Retirement Institute
National Association of Insurance and Financial Advisors
National Association of Mutual Insurance Companies