U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

August 7, 2023

Katie Johnson, Chair
Cynthia Amann, Vice Chair
Privacy Protections (H) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

Attn: Lois Alexander NAIC Market Regulation Manager
Via email: lalexander@naic.org

Re: Comments on Version 1.2 of the Draft Insurance Consumer Privacy Protection Model Law (#674)

Dear Chair Johnson and Vice Chair Amann:

The U.S. Chamber of Commerce ("Chamber") appreciates the opportunity to provide comments on Version 1.2 of the Draft Insurance Consumer Privacy Protection Model Law ("Model Law").[1] The Chamber represents industries from all sectors including the insurance and financial services sectors. As such, the Chamber has serious concerns that the proposed Model Law would directly and indirectly impact many parts of the economy. Accordingly, we respectfully request that the Working Group reassess the need for model insurance privacy legislation.

The data-driven economy has a profound positive impact on the economy by promoting public health, safety, and financial inclusion.[2] To properly protect the privacy of Americans and to prevent a confusing patchwork of laws while also fostering innovation, government must encourage uniformity and harmonization of data protection laws. For example, one study has shown that a patchwork of privacy laws would cost the American economy $1 trillion over ten years, and $200 billion of that burden would be shouldered by small businesses.[3] A patchwork of state laws would discourage businesses, particularly smaller ones, from innovating with data and 80 percent of small businesses maintain that losing access to data will harm their operations.[4]

[1] https://content.naic.org/sites/default/files/inline-files/Exposure%20Draft-Consumer%20Privacy%20Protection%20Model%20Law%20%23674%20as%20of%207-11-23_0.pdf
[2] https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf
[3] https://www2.itif.org/2022-state-privacy-laws.pdf
[4] https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf

Given the need to prevent a patchwork of differing and conflicting state laws, we support a federal national privacy law that establishes one privacy standard for the United States. However, we are concerned about the National Association of Insurance Commissioners' decision to pursue a novel model privacy law as states are already passing a consensus approach to comprehensive privacy laws. With the exception of California, twelve state legislatures have passed comprehensive privacy legislation that generally follows a model adopted by states like Colorado, Oregon, Texas, and Virginia.[5] The business community sees no need for novel model state privacy legislation that would be another layer of compliance for companies, particularly those that must comply with the consensus state privacy bills or the Gramm-Leach-Bliley Act.

For example, we offer the following ways in which novel or conflicting approaches in the Model Law would contribute to a state patchwork:

- **Basic Definitions**—The definitions in the Model Law regarding "biometric information," "consumer," "de identified," "personal information," and "sensitive personal data" do not align with existing state comprehensive laws. These definitions are fundamental to establishing uniformity in compliance for companies already having to operationalize existing state and federal laws. In addition, there is an inclusion of requirements for any "additional activities" throughout the Model Law, introducing an undefined term and additional unworkable requirements.

- **Publicly Available Information**—The Model Law would put in place restrictions on the sharing of publicly available information. This approach starkly contrasts with state laws that explicitly and wholly exempt this category of data from the scope of their bills.

- **Sensitive Data**—The Model Law would put in place prohibitions on the sharing of sensitive data. No state privacy bill has placed outright prohibitions on this practice. In fact, all states have provided for an opt-in model of sharing. This data can be particularly useful in providing services and products in an equitable manner.

- **Opt-in/Opt-out**—The Model Law is confusing as to what different processes must be followed regarding opt-in as opposed to opt-out requirements.

- **Notice Timing and Delivery**— The Model Law introduces prescriptive requirements for multiple disclosures and lengthy notices, including requirements for additional delivery as well as confirmations. This not only increases the burden to the client but also introduces additional cost while not embracing modernization.

[5] https://americaninnovators.com/2023-data-privacy/

- **Entity and Existing Law Exemptions**—The Model Law does not match the same exception list for entities not subject to the Model Law as the state comprehensive privacy law consensus approach. We urge the Working Group to reconsider its approach and to harmonize with current state law. Additionally, the Model Law does not provide exemptions for following laws like the Drivers Privacy Protection.

- **Joint Marketing**—Our members have raised concerns that joint marketing between financial institutions as authorized by the Gramm-Leach-Bliley Act may be restricted by new requirements.

- **Insurance Transaction**—Given the required contracts with third parties involved in "insurance transactions" the Model Law could potentially sweep in companies not traditionally regulated by insurance regulators.

- **Adverse Underwriting Decisions**—The Model Law would require notice and mandatory explanations to individuals for adverse underwriting decisions. No state comprehensive privacy law requires companies to provide notice for why they make business decisions on services or products provided. Additionally, such an approach could lead to costly litigation and business uncertainty.

- **Retention and Deletion**— The Model Law would provide prescriptive requirements concerning legacy systems which are extremely costly and burdensome. No other laws and regulations have provided such direction on licensees' technologies but have understood the ability for licensees to apply requirements in an applicable and risk-based manner, given protection and security has been applied.

- **Mandated Response Times**— The response times for access, correction, and deleted under the Model Law is only 15 days. This is significantly shorter than any other regime. Europe's General Data Protection Regulation provides 30 days for a response and various State regimes are generally 45 days. This inconsistent requirement is a significant burden on companies to provide the data required in an access request or provide consideration and a decision on a correction request. Additionally, the time for verifying the identity of the requester is included in that 15-day time frame.

The concerns highlighted in this letter are a non-exhaustive list of ways the Model Law does not align with current U.S. privacy law and could otherwise create unforeseen consequences throughout the economy. For this reason, we urge you to reconsider whether it is prudent to develop a novel model law that would have economy-wide impacts as opposed to approaches already taken by states and Congress.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce