April 29, 2020

NAIC Privacy Protections (D) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, MO 64106

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

Dear Chair Amann, Vice Chair Kreiter and Members of the Privacy Protections Working Group:

Thank you for soliciting stakeholder comments on your review of the *NAIC Insurance Information and Privacy Protection Model Act (#670)*. The American Council of Life Insurers respectfully submits the outline below per your requested format for submissions. We also provide the following very brief preliminary comments for your thoughts as the Privacy Protections Working Group continues its work.

As we mentioned in our remarks last December, we are proud of the fact that the insurance industry has traditionally been a conscientious and responsible guardian of customers' highly sensitive personal information. Our industry has appropriately managed consumers' confidential medical and financial information for decades. Appropriately, insurers 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 customers' 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.

Policymakers have responded to the privacy debate with varying proposals to provide consumers with greater transparency and control over the use of personal information, with California being the leading example. However, while lawmakers in California passed comprehensive new requirements for the entire business community, they did not harmonize the existing privacy requirements applicable to insurers. Among current insurance specific privacy laws in California are both the *NAIC Insurance Information and Privacy Protection Model Act* and the *NAIC Privacy of Consumer Financial and Health Information Regulation*. As a result of the lack of synchronization, the insurance industry is now burdened by a need to reconcile and comply with multiple laws and regulations ranging from longstanding requirements to sweeping new consumer privacy rules.

In addition to these sectoral requirements, insurers must ensure compliance with laws such as the Fair Credit Reporting Act ("FCRA"), the Driver's License Protection Act, the California Consumer Privacy Act ("CCPA"), the Online Privacy Protection Act, and the California Shine the Light law when doing business in California alone. For multi-state insurance carriers, the picture is even more complicated.

As you can see from the example above, insurers are uniquely affected by the confluence of general consumer privacy laws and our existing regulatory scheme. The consequences of differing, overlapping and sometimes conflicting requirements – as we are seeing play out in California with unclear scopes, definitions, notice requirements and consumer rights – may ultimately detrimentally impact our business models, particularly considering the types of data we collect, our legacy systems, and long history of data collection. Subjecting the insurance industry to conflicting or overlapping requirements, such as those in California, hurts rather than

helps consistency. We urge a cautious and deliberative approach to the review of Model #670, taking into consideration the challenges the industry is facing in California, to avoid unnecessarily complicating privacy law any further.

Setting aside the difficulties we face as an industry, differing state privacy approaches are confusing and frustrating to consumers, who are increasingly subject to divergent rights to control their personal information.

Questions for Regulators to Consider

- How do you envision the current insurance privacy regulatory system meshing with new comprehensive laws such as the California Consumer Privacy Act? How would changes to Model Act #670 interact with laws such as the CCPA?
- How will changes to Model Act #670 (which has been adopted in fewer than half of all states) interact with the Privacy of Consumer Financial and Health Information Regulation #672, which is adopted in some form in all states?
- How will insurance companies be able to compete with technology companies with differing rules on the use of personal information?
- How can we provide control and equal protections to all consumers with regard to their personal information no matter where they live or with whom they are doing business? In other words, provide consumers with legal transparency and the same level enforceable rights.
- How can we develop a regime that is robust and supports growth and innovation?
- How do we avoid consumer confusion over this already complex issue?
- How do we avoid the obstruction of the flow of data and impediments to interstate commerce?
- How do we prevent the distortion of competition (tech v. retail v. insurance)?

The collective theme for the questions above is that insurers should not be saddled with customized, industry specific privacy rules while the Amazons, Googles and InsureTechs have separate rules. An outcome in which we have the CCPA applying to some business, GLBA/Model regulation #672 adopted in all 50 states, and a revamped Model #670 incorporating GDPR and CCPA concepts adopted in some portion of states would be a fragmented and confusing system for consumer and companies.

It is with the context above we submit the following response to your request for your bulleted outline.

Outline Response:

We submit the following outline regarding the regulator comments to Model Act #670 per the request for an abbreviated format:

Preamble

- Flag for discussion later

Section 1. Scope

- Distinguish between lines of business (§1 A & B) – Flag for discussion later
- Review of definitions and alignment with other laws – Yes, we agree
- §1 D. – Not applicable

Section 2. Definitions

- Flag entire section for discussion later. If regulators are going to go through with this exercise, then taking a wholistic approach to the definitions is necessary.

Section 3. Pretext Interviews

- Compare to other anti-fraud definitions – Flag for discussion later

Section 4. Notice of Information Practices

- Notice at time of application – Flag for discussion later
- Elimination of exemption for annual notice if notice has been given in past 24-months – No, we disagree to any changes to this provision
- Disclosure of sources of information – Flag for discussion later
- Types and sources of personal information (§4 B (2)) – Flag for further discussion
- Types of data insurer may use (§4 B (3)) – Flag for further discussion
- Streamlining of certain disclosure requirements (§4 B (4)) – Flag for further discussion
- Disclosure of reports prepared by insurance support organizations (§4 B (6)) – Flag for further discussion
- Addition of CCPA/GDPR provisions to notice regarding restriction of use of personal information (§4 B (7)) – Flag for further discussion
- Abbreviated notice (§4 C) – No, we disagree with changes to this provision
- Permitting outsourcing notice responsibility (§ 4 D) – No, we disagree with changes to this provision
- Notice needs to be modernized – Flag for further discussion
- Electronic notice – Flag for further discussion
- Change from notice to consent to collect and use – No, we disagree
- Notice at renewal if there have been changes in the types of information collected, used or disclosed – Flag for further discussion
- Notice should include specific purposes for collecting the personal information and intended use – Flag for further discussion
- Disclosure without prior authorization if it's a "general business practice" – No, we disagree with changes to this provision
- Elimination of abbreviated notice – No, we disagree with the elimination of this provision

Section 5. Marketing & Research Surveys

- Alignment with CCPA/GDPR – Flag for further discussion

Section 6. Content of Disclosure Authorization Forms

- Addition of business purpose, categories of third parties with whom shared and for what purpose – Flag for further discussion
- Approval of Disclosure Authorization Forms – No, we disagree
- Opt-in for marketing – No, we disagree
- Change collected to disclosed (§6 F) – No, we disagree
- Add categories specified in Section 13 (Disclosure Limitations & Conditions) – No, we disagree
- Disclosure authorization timeframes (§6 G) – No, we disagree with changing timeframes
- Drafting note regarding the authorization disclosure form being superseded by other statutory requirements (§6 H) – No, we disagree

Section 7. Investigative Consumer Reports

- Flag for further discussion

Section 8. Access to Recorded Personal Information

- The terminology and concepts in Section 8 are antiquated. Regulators have identified many areas related to electronic communication and records that may need to be addressed – Flag for further discussion
- Charge for access – Flag for further discussion
- Inclusion of third-party vendors, InsureTechs, TPAs – Flag for further discussion

Section 9. Correction, Amendment or Deletion of Recorded Personal Information

- Addition of CCPA-type parameters (§1798.105) for denial of a deletion request – Flag for further discussion
- Addition of 'right to be forgotten' – Flag for further discussion
- Responsibility for correcting incorrect information – Flag for further discussion
- Inclusion of minors – Flag for further discussion

Section 10. Reasons for Adverse Underwriting Decisions

- 90-day response to lengthy – No, we disagree
- Specific reasons for adverse underwriting should track with HIPAA – No, we disagree
- Questions regarding oral basis for adverse underwriting decision – Flag for further discussion

Section 11. Information Concerning Previous Adverse Underwriting Decisions

- Delete Section 11 – Flag for further discussion

Section 12. Previous Adverse Underwriting Decisions

- Delete Section 12 – Flag for further discussion

Section 13. Disclosure Limitations and Conditions

- Deletion of requirement for written authorization for disclosure of personal information – Flag for further discussion
- Disclosure when "reasonably necessary" too vague – Flag for further discussion
- Disclosure to a medical institution or professional, comport with HIPAA – Flag for further discussion
- Disclosure to law enforcement – Flag for further discussion
- Reference to record retention and information destruction rules – Flag for further discussion
- Follow CCPA/GDPR – Flag for further discussion
- What about affiliate sharing provisions under GLBA, FCRA and the FACT Act?
- Opt-in instead of opt-out – No, we disagree
- Differing disclosure requirements for affiliates – Flag for further discussion
- Add provision prohibiting discrimination against a consumer who exercise their rights – Flag for further discussion

Section 14. Power of Commissioner

- Inclusion of third-party vendors under the authority of the commissioner – Flag for further discussion

Section 15. Hearings, Witnesses, Appearances, Production of Books and Service of Process

- Update definition of data and related information – Flag for further discussion

Section 16. Service of Process – Insurance Support Organizations

- Update methods and proof of service of process – Flag for further discussion

Section 17. Cease and Desist Orders and Reports

- No comment

Section 18. Penalties

- Tie penalties to an existing general penalties statute – Flag for further discussion

Section 19. Judicial Review of Orders and Reports

- No comment

Section 20. Individual Remedies

- Align with CCPA/GDPR – Flag for further discussion
- Inclusion of private cause of action – No, we disagree with the inclusion of a private cause of action

Section 21. Immunity

- Align with CCPA/GDPR – Flag for further discussion

Section 22. Obtaining Information Under False Pretenses

- Flag for further discussion

Section 23. Severability

- No comment

Section 24. Effective Date

- Effective date should be at least 2 years from enactment of the statute

Conclusion

In the midst of technological transformation, consumers and businesses need privacy standards that are coherent, and which provide a common understanding of safeguards. We believe regulators should avoid creation of a system which would provide differing consumer rights; differing levels of protections; fragmented implementation of consumer protections; and legal uncertainty. We believe that this complex issue warrants a comprehensive and deliberative review and we look forward to working with the Working Group as you continue your review.

Sincerely,

Kate Kiernan