Attached is the draft of the Consumer Privacy Protection Model Law (#674)

1. **Please provide your comments to Lois Alexander at lalexander@naic.org on or before April 3, 2023.**
2. **If you disagree with a provision in the draft model law, please:**
    a. **Provide specific reasons for your concerns, and**
    b. **Provide language that will address your concerns.**
    c. **If you want to discuss the draft model law with the group, please send an email to Lois Alexander and we will set up a meeting.**

The drafting group used the following principles to guide the drafting of the model law #674:

- **Existing NAIC Privacy Models--**The draft Model Law is intended to take the provisions and requirements of *NAIC Insurance Information and Privacy Protection Model Act #670 (Model 670)* and the *Privacy of Consumer Financial and Health Information Regulation #672 (Model 672)* updating and improving them. If the new model is adopted, it will supersede the two older models, which are approximately 40 and 30 years old, respectively).
- **Third Party Service Providers—**Initially, the drafting group took the position that insurance regulators should directly regulate third-party service providers. However, this position has evolved over time. After looking at the model as a whole, the drafting group decided this was not the correct approach. Consequently, the draft now provides for direct regulation of licensees and regulation of third-party service providers through any contract or agreement they hold with licensees. The residual jurisdiction that the draft model law retains over third-party service providers is essentially verbatim from Model #670. Because insurance servicing arrangements are increasingly prevalent and complex, it is important that state-based regulators retain some authority over those practices.
- **Data Minimization**—A licensee should only collect, process, share, and retain consumer information needed for insurance transactions, research, studies, and marketing and no more. To do otherwise, needlessly increases the risk of cyber events affecting both the licensee and the consumer. The draft model provides that licensees may retain consumers' personal information until it is no longer needed. De-identified data is not regulated under the draft model—we did not see any privacy concerns with such information. Furthermore, licensees may freely perform a variety of research and studies using aggregate, de-identified data. The draft Model does not regulate de-identified information because there are no privacy concerns associated with data that cannot identify an individual.
- **Consent**—The drafting group discussed this concept exhaustively. We decided that it was needlessly burdensome to require a consumer to give consent prior to collecting

information in connection with an insurance transaction. However, we do believe that consent is appropriate before consumers' sensitive information is shared with other entities and entities outside the jurisdiction of the U.S. where there may not be any privacy laws protecting such information.

- **Sale of Consumers' Personal Information**—In the draft, we decided that we should take a definitive line and prohibit licensees' from selling consumers' personal information. During our discussions with members of industry, we did not encounter any companies that sell consumers' information; the practice does not appear to be common. There is no similar prohibition on the purchase of consumers' information.

- **Transparency**—There should be transparency in the relationship between the licensee and the consumer with respect to a consumer's personal information—how and why it's collected, processed, shared, and retained.

- **Adverse Underwriting Decisions**--Because this model is going to replace Model 670, we had to address adverse underwriting decisions (AUDs). Notice and documentation of AUDs are important consumer protections that consumers and regulators will lose if Model 670 is repealed. The drafting group believes that these protections fit well into the concepts upon which the Working Group was charged with including in the draft model. In many cases, AUDs are based on personal information relating to the consumer; allowing the consumer to request the reasons for the AUD and the pieces of information upon which the AUD is based. If the decision was based upon inaccurate personal information, the draft Model Law provides that a consumer may request correction of the same via the processes contained in the Model. We feel that inclusion of AUDs is consistent with the concepts upon which we relied to draft the model.

- **Correction/Amendment**—Licensees are collecting, using, and retaining more of consumers' personal information than ever before. The drafting group took the position that if the licensee needs the information to conduct the business of insurance, it should be correct. You may have noticed that the drafting group removed the "right to delete" that Model 670 contains. We recognize that licensees need to keep information in various forms for longer than many other types of businesses.

- **Right to Forget**--The drafting group also discussed the principle of the "right to be forgotten" that is part of the state consumer data protection laws recently enacted. Ultimately, the group agreed that the insurance industry has a business need to retain information for longer than the gas station down the street. Instead, we developed a record retention provision.

- **State Consumer Data Protection Laws**--Additionally, we looked at the state consumer data protection laws for guidance. While we did not go as far as those laws do (the concept of "forgetting a consumer" would not work in the insurance context), we believe the approach of these state laws reflects the dangers and challenges facing us all with respect to the handling of consumers' personal information. Therefore, many of the concepts in the draft model are derived from these state privacy laws, which are among the most

current in the U.S.. We are also aware that certain positions taken in the model will have to be amended once we have the insurance industry's input; that is all part of the process.

- **Uniformity—**We were also guided in development of the draft model law by the protections and requirements that apply to protected health information under the Health Insurance Portability and Accountability Act (HIPAA). Thus, we included a safe harbor in the draft model law for those entities that comply with HIPAA.

- **Conversations with Individual Companies**--The drafting and editing groups had one-on-one conversations with six to seven life and health companies to discuss many of these concepts and to hear how those companies handle consumers' personal information. It was gratifying to us to learn that the policies and practices of those companies are consistent with the overall approach taken in the draft model.

  While no property/casualty (P/C) companies volunteered to speak to us during the initial round of meetings, we have since been contacted by four to five P/C companies with whom we will meet in February. The Working Group believes these meetings are very important to the process.