EVERSHEDS SUTHERLAND

THE Committee OF Annuity Insurers
www.annuity-insurers.org

**July 28, 2023**

Chair Katie Johnson (VA)
Vice Chair Cynthia Amann (MO)
2023 NAIC Privacy Protections (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, Missouri 64106

Sent via email to: lalexander@naic.org

**RE: Insurance Consumer Privacy Protection Draft Model Law #674 (Model #674)**

Dear Chair Johnson and Vice Chair Amann:

The Committee of Annuity Insurers (CAI or Committee)[1] appreciates the opportunity to submit the following comments to the 2023 NAIC Privacy Protections (H) Working Group (Working Group) on the exposure draft of Model #674 version 1.2 (published July 11, 2023) (the Revised Draft). We applaud the Working Group's continuing efforts on this complex and important issue and its commitment to continuing to work collaboratively over the coming months with consumer and industry stakeholders in order to craft effective and pragmatic enhancements to consumer privacy protections that are tailored to the insurance sector.

**OVERVIEW**

The CAI recognizes and appreciates the Working Group's efforts to respond to and reflect previous comments made by the CAI and others. The Revised Draft certainly represents a step in the right direction toward providing enhanced privacy protections to consumers in a way that is pragmatic and workable for licensees. That said, the CAI continues to have significant concerns regarding the Revised Draft, including issues we previously commented on as well as new issues arising from new language contained in the Revised Draft.

As revised, Model #674 would dramatically change the equilibrium that has been struck among insurance, banking and securities regulators regarding consumer privacy rights by placing much stricter limitations on insurance licensees' ability to process their consumers' data relative to the banking and securities sectors. This would put CAI members and all insurers at a competitive disadvantage in the broader marketplace for financial products, including by prohibiting their use of certain personal information even with the consumer's consent and reducing the ability of insurers to market products to consumers who may benefit from those products.

As you continue to work on the draft Model #674, we again urge you to be mindful of the balance between protecting consumers and enabling the smooth and efficient operation of insurance businesses that provide necessary and important financial protection and tools to those consumers. We also urge you to be mindful of the interplay between the various provisions of the Revised Draft and how they

[1] The Committee of Annuity Insurers is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 31 member companies represent approximately 80% of the annuity business in the United States. More information is available at https://www.annuity-insurers.org/.

may result in conflicting approaches to the same issue and unintended outcomes. To assist stakeholders, including the CAI, in responding to the Working Group's ongoing efforts, we also request that the Working Group provide additional commentary on the Working Group's thinking and intended approach to issues under consideration in the Revised Draft.

Our comments below focus on several significant aspects of the Revised Draft that CAI members believe warrant particular attention in this regard.

**COMMENTS**

**1. The data minimization limitations, including consent requirements for marketing, would limit the ability of licensees to compete in the marketplace and innovate in the future.**

**a. Limiting licensees to processing personal information for only statutorily permitted purposes is the wrong approach.**

The Committee recognizes and appreciates the changes made to Section 4 on data minimization and Section 5 on sharing limitations to expressly allow certain marketing activities, including the ability to market non-insurance financial products and services without obtaining consumer consent. That said, the problematic overall approach taken by Model 674 does not appear to have changed.

Sections 4 (Data Minimization) and 5 (Sharing Limitations) would still limit the ability of insurance licensees to collect, process, retain, or share personal information collected in connection with providing an insurance product or service to a narrow list of statutorily defined circumstances. Collecting, using, or sharing any personal information that cannot be tied back to an "Insurance Transaction" would be an "additional activity" and would require consumer consent. Additionally, Section 5(A) appears to further limit the purposes for which personal information may be collected in connection with an "Insurance Transactions" to only when "necessary" to carry out certain defined purposes related to an "Insurance Transaction".

This approach continues to be overly restrictive, and would inhibit innovation and flexibility in the insurance marketplace. Sitting here today, neither regulators nor licensees can hope to accurately identify and quantify the full scope and variety of activities that licensees conduct as part of their businesses today, nor how their offerings will evolve in the future. Accordingly, any list of permissible "Insurance Transactions" and related purposes for processing personal information defined in Model 674 will inevitably be overly narrow as the market continues to develop. Additionally, fixing or updating the list would require legislative action on a state-by-state basis, an exceptionally difficult and slow process. Accordingly, this approach will inevitable hamstring the insurance industry, suppressing innovation and harming its ability to compete in the broader financial service marketplace.

*CAI Recommendations.* We request that licensees be permitted to collect, use and share personal information consistent with their privacy disclosures, without making artificial distinctions between an insurance transaction and "additional activities", subject to certain opt-out rights. Consent to collect, use and share personal information should not be required. Collection of personal information should still be minimized to that data that is reasonably necessary for the disclosed purposes for which the personal information is collected. This approach would be consistent with the approaches taken under the California Consumer Privacy Act and other existing and emerging US and international privacy laws.

**b. Licensees must be able to share privileged information with certain non-affiliated third parties.**

As drafted, Section 5(B) of the Revised Draft would require licensees to obtain consumer consent to share "privileged information" with any non-affiliated third party. "Privileged Information" is defined to include any personal information that relates to a claim for insurance benefit or any civil or criminal proceedings involving a consumer. There is no exception provided for sharing information with outside counsel, independent claims adjusters, or similar third parties. Licensees clearly need to be able to share information with such third parties in order to engage in normal day-to-day operations, including as necessary to pursue or protect their legal interests.

*CAI Recommendations.* Section 5(A) should be amended to provide that consent is not required where privileged information is shared with a third-party service provider. We suggest doing so through the addition of a new section that specifically permits licensees to share personal information with third-party service providers to the extent reasonably appropriate in connection with the services being provided.

**c. Clarify the limitation on third parties further sharing personal information in connection with additional activities.**

Section 5(C)(2)(a) appears intended to limit third parties who receive personal information in connection with providing additional activities from further sharing the information. However, as currently drafted this section would prohibit any "person" conducting additional activities from further sharing personal information, which would include licensees directly providing such additional activities. This would effectively prohibit licensees from using third-party service providers in connection with additional activities, even with consumer consent.

*CAI Recommendations.* This section should be clarified to refer to a "third party" instead of a "person".

**d. Consumers should be empowered to decide how their personal information can be used and shared.**

Section 5(C)(2)(b) of the Revised Draft would prohibit any sharing of "Sensitive Personal Information" in connection with additional activities involving marketing a non-insurance or non-financial product or service. This appears to be a flat prohibition, regardless of consumer intent. Additionally, while this provision appears to only prohibit sharing the data, Section 6(C)(4) suggests it is meant to operate as a broader prohibition on even internal uses of Sensitive Personal Information for marketing of additional activities. Instead of empowering consumers to choose how their personal information is used and shared, this provision would make the decision for them. It would also prevent licensees from engaging in normal marketing practices that help them to effectively market beneficial products in a crowded and competitive market.

Similarly, Section 5(E) appears to be a broad prohibition on selling consumers' Personal Information, regardless of consumer intent or consent.

*CAI Recommendations*. Processing or sharing personal information should never be flatly prohibited. Rather, consumers should be empowered to opt-out of the sharing of sensitive personal information or selling of personal information, subject to certain exceptions.

**2. Revise sections where consumer consent appears to be required for opt-out rights.**

The CAI appreciates that the Working Group has responded to previous comments made by the CAI and others by incorporating language in the Revised Draft that seems to move from a consent based approach to an opt-out approach for marketing and joint marketing activities. However, there are several sections of the Revised Draft that seem to cut against this approach and make it unclear as to whether some form of consent or authorization remains required.

For example, Section 5(A)(14) defines what licensees must do to engage in joint marketing, which states that consumers must be provided the right to "opt-out". However, Section 5(A)(14)(c) appears to also require an "authorization" that complies with Section 6 (Consumer's Consent). Requiring consent or authorization of any kind to engage in marketing is diametrically opposed to an "opt-out" approach. It is therefore unclear as currently drafted what is required for licensees to use personal information for marketing, and whether the law takes an opt-in or opt-out approach. The same issue exists in Section 5(A)(15) regarding what is required to engage in marketing.

Similarly, Section 6(A) seems to indicate that consumer consent could be required in connection with both opt-in and opt-out rights, stating "Where the consumer's consent . . . is required by this Act, whether opt-in or opt-out, . . ." This language is self-contradictory. Any approach that requires consumer

consent or authorization is not an opt-out requirement, but rather an opt-in requirement. A similar issue exists in Section 6(B).

*CAI Recommendations.* The Revised Draft should be further revised to clarify that consent is not required in connection with marketing or joint marketing activities, and rather that an opt-out approach is being taken. At a minimum, subsections (c) should be deleted from both Sections 5(A)(14) and (15). Additionally, the reference to "whether opt-in or opt-out" should be deleted from Sections 6(A) and (B).

**3. Clarify that de-identified information is not personal information and is excluded from the restrictions and requirement of Model 674.**

The Revised Draft includes conflicting language regarding how de-identified information is treated under Model 674 and causes confusion over the extent to which de-identified information is subject to regulation under Model 674. The Definition of "Personal Information" in Section 2(DD) clearly states that de-identified information is not personal information. We believe this reflects the Working Group's intent, and is appropriate since the use of de-identified information does not pose privacy risks to consumers.

However, Section 5(D) appears to limit the ability of licensees to collect, process, retain, or share de-identified personal information to only "as necessary in connection with insurance transactions and additional activities". This is incongruous and inconsistent with the definition of personal information, and would regulate de-identified data as a subset of personal information.

Similarly, several provisions in the Revised Draft would require that personal information be entirely deleted in various circumstances, without allowing for de-identification in lieu of deletion. For example, Section 7(C)(1) would mandate that personal information be "deleted" within 90 days of a determination that the personal information is no longer needed for certain specified purposes. The definition of "delete" in Section 2(M) states this means such data must be "permanently and completely eras[ed]." It does not allow for de-identification. Indeed, Section 7(C)(2) suggests that de-identification is only permissible where deletion is not feasible. This approach would lead to the incongruous result that the same de-identified information would be permissible for licensees to maintain if it was collected in a de-identified manner, but would be impermissible to keep if it was collected in an identifiable form and later de-identified. It is unclear what regulatory purposes this approach would serve.

*CAI Recommendations.* We request clarification that a licensee could de-identify personal information in lieu of deleting it, as such data would no longer be personal information. This could be accomplished by amending the definition of "delete" to allow for de-identification and by deleting Sections 5(D) and 7(C)2.

**4. The requirements for enhanced third party oversight and contracting requirements would still adversely limit the ability of licensees to hire top service providers.**

The Revised Draft contains largely the same third party oversight provisions as previously proposed and continues to raise issues of significant concern. Section 3(B) would continue to require third-party service providers to agree to "abide by the provisions of this Act" and to require them to implement appropriate measures to "comply with the provisions of this Act". As drafted, this appears to be an attempt to exercise long-arm jurisdiction over third-party service providers through contractual requirements that the licensee must impose. As we previously commented, many service providers will not be willing to agree to comply with a law that would not otherwise apply to them. In practice, these requirements would serve only to alienate quality service providers from serving the insurance sector, and limit the ability of licensees to assess and manage the privacy risks posed by third-party service providers. We reiterate our comments made on this issue in our previous comment letter dated April 3, 2023 and maintain that licensees should be empowered to pick the best vendor overall, not just the vendors willing to agree to certain contractual language.

Section 3(G) also carries over an additional issue from the previous draft of Model #674 by requiring that contracts with third-party services providers require that both the licensee and service provider must comply with consumer "directives". As drafted, both parties would be prohibited from "collecting,

processing, retaining, or sharing the consumer's personal information in a manner inconsistent with the directive of the consumer", regardless of whether that directive goes beyond the consumer rights otherwise provided in Model # 674. This would be virtually impossible for licensees and service providers to comply with in practice, and would be extremely burdensome.

*CAI Recommendation.* Instead of applying a one-size-fits-all approach that will limit the ability of licensees to engage the best service providers in the market, Model #674 should be revised to take a risk-based approach. The CAI recommends that the Model require licensees to conduct appropriate due diligence and oversight of all third party service providers that process personal information, and require licensees to negotiate appropriate contractual protections based on the assessed risk of the service provider. The Model should not specify what those contractual protections would include beyond limiting the service providers' ability to use, share or disclose personal information for purposes other than providing the services and requiring the third party's cooperation when consumers exercise their rights to data correction and deletion.

Section 3(G) should be deleted. Alternatively, at minimum, Section 3(G) should be revised to clarify that parties must honor a consumer's decision to exercise rights provided under Model # 674, not comply broadly with any directive submitted by a consumer.

**5. Key definitions need clarification and refinement.**

**a. The definition of "consumer" should be clearly focused on personal information collected in connection with an insurance transaction.**

As currently drafted, the definition of a "consumer" in the Revised Draft is extremely broad, and would appear to include virtually any individual whose personal information a licensee collects. Section 2(I) currently defines "consumer" to include information on any individual "whose personal information is used, may be used, or has been used in connection with an insurance transaction. Including any individuals whose information could possibly be used ("may be used") in connection with an insurance transaction expands the definition significantly with no clear boundary. For example, this definition could be interpreted to apply to employee information, business partner information, and other information that is not actively collected in connection with an insurance transaction, since any such information could potentially be used in connection with an insurnace transaction in the future. This drafting of the definition would seem to be at odds with other provisions of Model # 674, which are appropriately focused on protecting actual insurance customers rather than any personal information that happens to be collected by a licensee.

*CAI Recommendations*. The definition of "Consumer" should be aligned with the existing definition in Model # 672.

**b. The definition of "personal information" should be clarified.**

As currently drafted, the definition of "personal information" under Section 2(DD) would be limited only to the specific types of personal information listed under Section 2(DD)(1). This drafting would appear to contrast to the apparent intent of the language otherwise included in Section 2(DD) defining personal information as "any individually identifiable information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a consumer . . . ."

Additionally, there appears to be a typo in the definition, as it states that the definition applies to consumer information "that is by or on behalf of a licensee . . . ." A word appears to be missing from this phrase, and it is unclear what it is meant to convey.

*CAI Recommendations*. The definition of personal information should be revised and clarified, including to clearly indicate whether the list of items in Section 2(DD)(1) are meant to be an exclusive or illustrative list of what constitutes "personal information".

**c. Define "additional activities".**

The concept of "additional activities" is central to the current Revised Draft of Model 674. However, this key term is not defined. Based on how it is used within the Revised Draft, it appears intended to include any activity that is not defined as an "Insurance Transaction". To the extent the concept of "additional activities" is retained in future drafts, the term should be clearly defined. However, we reiterate that consent should not be required to collect or use information consistent with privacy disclosures made to consumers.

**d. Amend the definition of "personal information" to exclude "publicly available information".**

Unlike NAIC Model #672 Section 4(T)(2)(b), which excludes publicly available information from the definition of "personal information" in a manner similar to other state privacy laws, the Revised Draft does not explicitly exclude "publicly available information" from its scope. Rather, it restricts or adds requirements to the use of "publicly available information" throughout the draft, such as in Section 3(C), which permits a licensee to share "publicly available information" with a third party service provider only to the extent necessary to provide the service requested by the consumer. Similarly, new language in Sections 12 and 13 would require consumers to submit verifiable requests to access the consumer's personal and publicly available information in the possession of a licensee or its third-party service providers. Including "publicly available information" in this privacy law would be unprecedented, overly burdensome and detract from the purpose of privacy laws, which is to protect the privacy of private personal information.

*CAI Recommendations.* The scope of the requirements of the Revised Draft should be restricted to "personal information," and "publicly available information" should be explicitly excluded from the definition of "personal information." All references to "publicly available information" that impose additional restrictions or burdens on licensees should be deleted.

**e. Clarify the definition of an "insurance transaction".**

As currently drafted, the definition of "insurance transaction" under Section 2(V) appears to contain language that would result in unintended consequences. The first sentence of the definition provides that an insurance transaction is any transaction "by or on behalf of a licensee and its affiliates" (emphasis added). As drafted, this would mean that any of the specific transactions listed in the definition that follow this phrase would only qualify as insurance transactions if they are provided by both the licensee and its affiliates; the same transaction provided just by the licensee would not qualify. We do not believe this is the intended meaning.

Additionally, Subsection 2(V)(7) appears intended to provide flexibility for licensees to process personal information for short-term transient uses. However, as drafted the provision appears to enact additional limitations on the ability of licensees to engage in common marketing practices that would otherwise be permissible under the Revised Draft. Additionally, it does not expressly state that it is referring to the short-term, transient use of personal information; it simply refers to "short-term, transient use."

*CAI Recommendations.* The definition of "insurance transaction" should be reviewed and revised to clarify that an "insurance transaction" includes transactions or services provided by licensees or their affiliates, and to broadly permit short-term, transient uses of personal information.

**6. The limits on data retention in Section 7 should be revised to allow more flexibility.**

**a. Permitting retention of personal information only for the duration of an insurance transaction with the consumer should be modified to permit retention for any reasonable business purpose, as disclosed in the privacy notice.**

Revised Section 7(A)(1) would permit retention of personal information "as necessary" for "the performance of any insurance transaction with the consumer", after which the data must be deleted.

However, a retention scheme that relies on transactions with consumers fails to allow licensees to retain personal information received from affiliates and other financial institutions for legitimate business purposes, such as joint marketing. For example, once a single joint marketing campaign has been completed and the personal information used in connection with that campaign is no longer strictly "necessary" for purposes of that campaign (an insurance transaction), a licensee would be required to delete that personal information even if it will just need to gather the information again in the future for additional or limited campaigns.

*CAI Recommendations.* This provision should be modified to allow licensees to retain personal information for any reasonable business purpose, and as disclosed in their privacy notice.

**b. An annual review of "all consumers' personal information in its possession" is highly burdensome and should be changed to a review by category or type of personal information**

Revised Section 7(B) would require a licensee to annually review its data retention and "review all consumers' personal information in its possession" to determine whether the purposes for which the personal information was retained still remain. As drafted, licensees would be required to review all of the actual consumer personal information in its possession, as opposed to conducting a broader assessment of the types and amounts of personal information it retains. The annual review of all consumers' personal information in its possession is highly burdensome and unwarranted.

*CAI Recommendations.* Section 7(B) should be revised to clarify that the requirement is to annually review the type and amount of personal information in the licensee's possession, not specific personal information.

**c. The 90-day period to completely delete a consumer's personal information should be extended.**

Revised Section 7(C)(1) provides that once a licensee has determined that the consumers' personal information is no longer needed, then the licensee shall completely delete all the consumers' personal information within 90 days. We had previously commented that the 90-day time period to completely delete all personal information is too short and impractical, given the number of systems on which the personal information can be retained, including systems such as application, underwriting, operational, claims, distribution and other systems. Personal information will also be retained on backup systems, which present special issues and may be accessible only on a quarterly basis. Moreover, given the length of time that personal data must be retained, some consumer data may be in paper files that are archived and difficult to access.

The current version of the Model Law does not add flexibility on this point, other than to add new language that gives the commissioner the discretion to grant exceptions for good cause shown. Practical questions remain, however, regarding the severity of this 90-day requirement and regarding which commissioner would grant the exception, especially if one or more commissioners other than the commissioner in the insurer's state of domicile can weigh in on this issue.

*CAI Recommendations.* Section 7(C)(1) should be revised to provide an annual deletion period, which would be more manageable and permit insurers to include deletion of personal information in their periodic cycles of system maintenance.

**d. The requirement to replace legacy systems within 10 years if they do not permit targeted disposal is highly prescriptive and costly without taking collateral consequences into account. Compensating controls should be permitted as an alternative to legacy system replacement.**

Section 7.C.(2) of the Revised Draft would require a licensee that cannot de-identify or delete consumers' personal information from a system to replace the system within 10 years and to annually report to their domestic regulator on their progress in completing the project within those 10 years.

The commissioner has discretion to grant exceptions for good cause. Assuming the revised Model # 674 is ultimately adopted broadly, as currently drafted a licensee would be required to obtain an exception from each state commissioner in order to avoid having to migrate away from an existing legacy system.

The reality of migrating off of a legacy system in practice is extraordinarily complex, time consuming, and astronomically expensive. The process would easily take more than a decade to complete for some systems, and result in large costs that would necessarily be passed on to consumers. Part of the reason for this complexity and difficulty is that legacy systems are not stand-alone systems, but rather are deeply entrenched and enmeshed in licensees' information technology infrastructure. Migrating away from a legacy system would mean: (1) peeling back decades of custom and iterative software development and system design to disentangle the legacy system from the overall IT architecture; (2) migrating huge volumes of data to the new system in a way that transforms data from legacy formats to formats used by newer systems while ensuring consistency and fidelity in the data set; (3) integrating the new system with hundreds of other existing systems that interact with and depend on the existing legacy system to function; and (4) manage to complete all those tasks without disrupting ongoing business operations.

The task is enormous, comes with large amounts of operational and business interruption risk, and should not be taken lightly. We do not believe mandating such projects broadly across the insurance sector is an appropriate remedy to concerns about data minimization. Moreover, licensees are already subject to cybersecurity requirements, which require the adequate protection of personal information stored on legacy systems. Licensees have spent millions of dollars implementing compensating cybersecurity and privacy controls on their legacy systems, controls that are designed to appropriately protect consumer personal information held on such systems in satisfaction of existing NAIC and state standards. We do not believe mandating migration away from legacy systems is the appropriate remedy for addressing the cybersecurity risks of legacy systems.

*CAI Recommendations.* The proposed requirement to migrate away from legacy systems goes beyond the purview of privacy and what a privacy law is intended to accomplish. We respectfully submit that Model #674 is not the venue for addressing this issue. Instead, the CAI requests that this requirement be removed and that flexibility be provided to address legacy systems issues through the development and approval of appropriate compensating controls.

**7. The delivery of the notice of consumer privacy protection practices ("notice of privacy practices") in Section 8 should be revised and made more flexible.**

**a. The requirement to provide a notice of privacy practices when a licensee or third-party service provider first collects the personal information of a consumer is unworkable and should be revised.**

As currently drafted, revised Section 8(B)(1) would require a licensee to provide an initial notice of privacy practices to the consumer at the time the licensee, directly or through a third-party service provider, first collects, processes or shares the consumer's personal information in connection with an insurance transaction or additional activity. This provision is unworkable on several levels.

For example, assume the licensee is planning a digital marketing campaign and has obtained information about a consumer that does not include a street address. In such cases, how is the licensee going to send an initial notice of privacy practices to a consumer at the time the licensee first collects the consumer's information if the licensee has not obtained a mailing address for the consumer from the marketing agency? Note that Section 11(B)(3) would require the notice of privacy practices to be mailed to the individual at the time of collection.

Additionally, under the current language, the trigger for sending the notice of privacy practices is when the insurer receives the marketing leads from a third-party marketer, not when the licensee or its agent contacts the consumer. However, the licensee would not know whose information it is collecting until it receives the personal information, and therefore it would be impossible to comply with the

requirement to provide notice at the time the data is collected. Additionally, requiring every licensee that would market to a consumer to deliver a privacy notice would create a deluge of privacy notices to consumers that would render the notices ineffective and annoying.

*CAI Recommendations.* A more effective and relevant approach would be to revise Section 8(B)(1) so the sending of the notice of privacy practices was triggered when the licensee is first in direct contact with a consumer and can obtain the information necessary to send the privacy practices notice.

**b. The requirement on when to send a notice of privacy practices to a beneficiary should be clarified.**

New language in revised Section 8(B)(1) states that the term "consumer" includes a third-party claimant or beneficiary in connection with a claim under an insurance policy. However, there is ambiguity regarding when the initial notice of privacy practices must be sent to third-party claimants and beneficiaries. Often, an insurer licensee first collects a beneficiary's name and possibly contact information at the time the insured applies for an insurance policy or contract. But the actual processing of a claim likely will occur much later.

*CAI Recommendations.* The Committee requests that Section 8(B)(1) be revised to clarify that a notice of privacy practices must only be delivered to beneficiaries at the time a claim is filed with the licensee.

**8. The requirement that the notice of privacy practices list the persons who received the consumer's personal information should be deleted. In the same vein, consumers should not be given the right, in the notice of privacy rights, to obtain the identification of all persons who have received the consumer's personal information.**

Revised Section 9(A)(5) continues to require that the notice of privacy practices state that a consumer may obtain a list of persons with whom the licensee or its third-party service provider has shared the consumer's personal information in the three previous calendar years. Because the term "person" is defined to include individuals, this would require licensees to track and maintain a list of every individual, internal or external, that processes a particular individual's personal information. We commented in our previous letter that this provision would be extremely costly, onerous and difficult to manage, while providing the consumer with little, if any, benefit.

Similarly, new Section 10(B)(e) would require a licensee to send a privacy rights notice to each consumer with whom the licensee has an ongoing relationship, giving the consumer the right to obtain "the identification" of all persons who have received the consumer's personal information in the past three years. As drafted, this requirement would be extremely burdensome, as noted above, and serve no clear purpose.

*CAI Recommendations.* The Committee reiterates its previous request that Section 9(A)(5) be generalized so that the licensee would be required to give an indication of the categories of third parties with whom the consumer's personal information was shared, not the names of individuals.

The Committee also requests that Section 10(B)(e) be generalized to provide notice of the types or categories of third parties with whom a consumer's personal information has been shared.

**9. The delivery requirements for the notice of privacy practices and the notice of privacy rights should be symmetrical.**

Revised Section 8(C) requires that the notice of privacy practices be delivered only when the privacy protection practices of the licensee change. But new Section 10(C) requires that the notice of privacy rights be provided to the consumer at least once every year, which in many cases would require the notice to be physically mailed. This new requirement would be costly, would be inconsistent with the revised approach that Congress has taken to delivery of privacy notices, and would be of limited utility

to the consumer, especially since the notice of privacy rights would be posted on the licensee's website and always available.

*CAI Recommendations.* The Committee requests that the annual delivery requirement for the notice of privacy rights and the requirement for delivery of updated notice of privacy practices be revised to allow that website posting of the notices satisfies the requirements for delivery of both the notice of privacy practices and the notice of privacy rights.

**10. Delivery of initial notices required by the Act should be more flexible.**

While the Revised Draft has added some flexibility for delivering notices required by the Act, it would still generally require notices to be mailed in hardcopy as the default approach. This is out of step with a modern approach to delivering notices. We reiterate our previous comments on this issue.

*CAI Recommendations.* The Committee requests that further flexibility be provided to allow licensees to send initial notices by default in the way that the licensee generally engages with that consumer. This approach, consistent with the approach taken in the CCPA, would allow a consumer who frequently uses the licensee's website to receive the initial privacy notices electronically, unless the consumer requests delivery in another way.

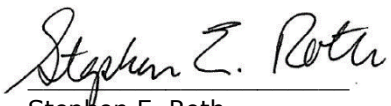
We want to express our deep appreciation for the opportunity to comment on draft Model #674, and we hope that you find these comments helpful at this stage. Please do not hesitate to contact us if you have any questions.

Sincerely,

**For The Committee of Annuity Insurers**

Eversheds Sutherland (US) LLP

By:



Stephen E. Roth
Mary Jane Wilson-Bilik
Alexander F. L. Sand
Eversheds Sutherland (US) LLP

EVERSHEDS SUTHERLAND

THE Committee OF Annuity Insurers
www.annuity-insurers.org

**April 3, 2023**

Chair Katie Johnson (VA)
Vice Chairs Cynthia Amann (MO) and Chris Aufenthie (ND)
2023 NAIC Privacy Protections (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, Missouri 64106

Sent via email to: lalexander@naic.org

**RE: Insurance Consumer Privacy Protection Draft Model Law #674 (Model #674)**

Dear Chair Johnson and Vice Chairs Amann and Aufenthie:

The Committee of Annuity Insurers (CAI)[1] appreciates the opportunity to submit the following comments to the 2023 NAIC Privacy Protections (H) Working Group (Working Group) on the exposure draft of Model #674. In providing our comments at this stage, we applaud the Working Group's efforts to date on this complex and important issue, and its commitment to continuing to work collaboratively over the coming months with consumer and industry stakeholders in order to craft effective and pragmatic enhancements to consumer privacy protections that are tailored to the insurance sector.

**OVERVIEW**

While the CAI recognizes and supports the importance of making tailored updates to the privacy rules governing the insurance sector, we are concerned that the current draft of Model #674 would meaningfully limit the ability of the insurance sector to compete within the broader financial services markets. The insurance industry, along with the banking and securities industries, comprise the three main branches of the financial services sector in the United States. These three branches are highly interconnected in providing services to consumers and all three branches have been subject to largely consistent rules under the Gramm-Leach-Bliley Act (GLBA) regarding the privacy rights that they offer to those consumers.

As proposed, Model #674 would dramatically change this equilibrium by placing much stricter limitations on licensees' ability to process their consumers' data relative to the banking and securities sectors. This would put CAI members and all insurers at a competitive disadvantage in the broader marketplace for financial products, including by prohibiting their use of certain personal information even with the consumer's consent; increasing costs for insurers by reducing their access to offshore service providers; and reducing the ability of insurers to market new products, even to existing consumers.

As you continue to work on the draft Model #674, we urge you to be mindful of the balance between protecting consumers and enabling the smooth and efficient operation of insurance businesses that provide necessary and important financial protection and tools to those consumers. Consumers understand that licensees need to collect personal information to provide them with the

[1] The Committee of Annuity Insurers is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 31 member companies represent approximately 80% of the annuity business in the United States. More information is available at https://www.annuity-insurers.org/.

financial products and services they request and to operate their businesses. We suggest that Model #674 should be tailored to the needs of the insurance sector specifically and to reflect consumer expectations in our industry. Our comments below focus on several significant aspects of the draft Model that CAI members believe warrant particular attention in this regard.

**COMMENTS**

1. **The data minimization limitations, including consent requirements for marketing, would limit the ability of licensees to compete in the marketplace and innovate in the future.**

Section 4 of the Model Law on "Data Minimization and Sharing Limitations" would limit the ability of insurance licensees to collect, process, retain, or share personal information collected in connection with providing an insurance product or service to a few narrow circumstances. This would include only being able to use data for marketing or internal research purposes (defined as "additional permitted transactions")[2] with prior express consent. Section 4 would prohibit any use of the information that does not fall under the definitions of an "insurance transaction" or "additional permitted transactions." This approach sets narrow limits on the purposes for which data may be used, without providing consumers the ability to consent to additional uses. Taking this approach would disrupt current business practices and create additional costs that would necessarily be passed on to consumers. It would also limit the ability of the insurance industry as a whole to innovate, since the use of personal information would be limited to only the seven enumerated uses.

We are also concerned about the breadth of Section 4(G) as proposed, in that it broadly prohibits any licensee from collecting processing, retaining, or sharing any personal information "in a manner inconsistent with the direction of a consumer . . . ." While it is unclear what the intent of this provision is, as drafted it would subject licensees and their ability to conduct business to the whims of each consumer. For example, a consumer could direct a licensee to only process their personal information for claims or marketing on Tuesdays and the licensee would be bound by that direction. This provision would also allow consumers to constrain the ability of licensees to retain their data, thereby creating a shadow deletion right within the Model. This provision should be deleted.

The requirement to obtain affirmative consent prior to using personal data for marketing to a licensee's own existing customers, would be particularly disruptive to current business operations. It would also functionally prohibit joint marketing with trusted financial institutions and limit the ability of licensees to inform consumers of the beneficial products and services they may need. Consumers may not take the time to provide marketing consent, not because they are necessarily opposed to receiving marketing but because they would not take the extra step necessary to provide consent. This would upend the basic business model of how many licensees market their products, hampering their ability to grow and maintain their businesses.

Because the restrictions of the draft Model are stricter than any other current or pending US privacy law (such as the California Consumer Privacy Act), including those that govern other financial services sectors, it would place the insurance industry as a whole at a competitive disadvantage with competing non-insurance financial products. For example, SEC-regulated broker-dealers and investment advisors that sell both annuities and competing non-insurance products (such as mutual funds or CDs) would be able to market the non-insurance product to a consumer readily, but would require consent to market an annuity product that may be a better fit to the same consumer. This imbalance would mean that broker-dealers and advisers would be more likely to offer non-insurance products to consumers, and create an asymmetry of information in the marketplace that would function to drive consumers away from insurance products that may better meet their needs. The CAI

[2] "Additional permitted transactions" means "collecting, processing, retaining or sharing a consumer's personal information, with the consumer's consent, for: (1) marketing purposes; or (2) research activities not related to rating or risk management purposes for or on behalf of the licensee." Section 3.B.

supports providing tailored privacy enhancements to insurance consumers, but suggests that it can be done without affecting the competitiveness of the insurance industry.

The rational underlying modern privacy regulation is based on two basic tenets: (1) consumers should be able to understand where their personal information goes and how it will be used; and (2) consumers should be able to exercise control over their personal information. We suggest that a revised version of the Model could achieve these goals without affecting the ability of licensees to compete in the market or innovate for the future.

*CAI Recommendations*. Instead of narrowly defining the permitted purposes for which personal information may be used, the Model should be revised to empower consumers to choose how their personal information may be used by exercising opt-out rights, and to allow purely internal uses of personal data.

To that end, the data minimization restriction should be limited to requiring that any collection, use, and processing of personal information must be reasonably necessary and proportionate to achieve the disclosed purposes for which it was collected. Separately, consumers should be able to opt-out from having their personal information used to market to them, or shared with non-affiliated third parties other than as necessary to administer a requested service (consistent with current Model #672). Purely internal uses of personal information that are properly disclosed should be permissible. We believe this approach would appropriately balance the interest of licensees in operating their businesses and offering beneficial insurance products into a competitive market with the rights of consumers to exercise control over their personal information.

**2. The prohibition on using and sharing sensitive personal information for marketing and research, even if the consumer consents, is overly restrictive.**

Section 4.E.(2)(b) of draft Model #674 would prohibit the sharing[3] of "sensitive personal information"[4] for marketing or any other "additional permitted transaction," even if the consumer consents to such sharing and use. It is common practice to use sensitive personal information to enhance digital marketing. Because the definition of sensitive personal information is so broad (it is similar to the definition found in the California Privacy Rights Act), the prohibition on the use of sensitive personal information in marketing would put insurers at a competitive disadvantage relative to other financial institutions' marketing activities that are not similarly constrained. This section would also limit the kinds of research an insurer can undertake to understand its business, including internal research into the impacts that certain insurance practices are having on various protected classes.

No other privacy law in the United States flatly prohibits the use of sensitive personal information in advertising or research. For example, the California Consumer Privacy Act requires that consumers be given notice and the opportunity to opt-out of the use of their sensitive personal

[3] "Sharing" is defined broadly to include "disclosing, disseminating, making available, releasing, renting, transferring, selling or otherwise communicating by an means a consumer's personal information…" Section 3.LL.

[4] "Sensitive personal information" is defined broadly to mean "information that reveals (i) a consumer's social security, driver's license, state identification card, or passport number; (ii) a consumer's account log-in or financial account, debit card or credit card numbers in combination with any required security or access code, password, or credentials allowing access to an account; (iii) a consumer's precise geolocations; (iv) a consumer's racial or ethnic origin, religious or philosophical beliefs; (v) union membership; (vi) the contents of a consumer's personal mail, personal email, and personal text messages unless the person in possession is the intended recipient of the communication; (vii) a consumer's genetic data; (viii) a consumer's sex life or sexual orientation; (ix) a consumer's citizenship or immigration status; (x) a consumer's health information; or (xi) a consumer's biometric information." Section 3.KK.

information for marketing. Similarly, no other U.S. privacy laws prohibit the use of sensitive personal information for research purposes.

Section 4.E.(2)(b) of Model #674 would also prohibit the sharing of sensitive personal information with affiliates for marketing purposes, even if no consideration passes between the parties. However, Section 4.I. of Model #674 contains one exception to the affiliate sharing prohibition. That section acknowledges the federal preemption language found in Section 625 (b)(1)(H) and (b)(2) of the Fair Credit Reporting Act ("FCRA") that prohibits the laws of any state from imposing any requirement or prohibition on select provisions of the FCRA. Those sections in turn reference FCRA's Section 624 Affiliate Sharing that, in effect, requires companies to (a) provide prominent disclosure to consumers that information about them in a consumer report may be communicated to an affiliate for marketing purposes and (b) give consumers a simple method for opting out of such marketing.

*CAI Recommendation*. Section 4.E.(2)(b)of Model #674 should be revised and brought in line with other privacy laws enacted at the federal or state level.

**3. The prohibition on processing personal information outside the United States without obtaining consumer consent would adversely limit the ability of licensees to choose the best service providers and would increase costs for consumers.**

Section 4.C. of the draft Model would prohibit licensees from sharing personal information with, or collecting or processing personal information through, an entity outside of the United States. Because it is unlikely that licensees would be able to obtain consent from all or even most consumers as a practical matter, this provision would function as a general prohibition on processing personal information outside of the US, including through domestic vendors. As a result, this requirement would disrupt existing business operations and relationships, triggering costs to create on-shore alternatives to existing offshore vendors. These costs would necessarily be passed on to consumers. It would also limit the ability of licensees to use cloud-based vendors and otherwise choose the best available service providers in the market, since many service providers simply do not allow for customers to limit data processing only to the US.

There are alternative means to protect consumers without limiting the ability of personal data to be processed outside of the U.S. The use of offshore vendors to process personal information is a common business practice that provides a range of consumer benefits, including enabling extended hours of customer support, reduced costs, and increased system resilience. Requiring consumer consent also would not directly address the risks posed by offshore data processing. Privacy laws like the EU GDPR that do establish limitations on transferring data to an outside jurisdiction do so to avoid offshore processing being used to avoid complying with onshore privacy requirements. To that end, the GDPR does not require consent to allow offshore processing or otherwise prohibit offshore processing, but rather establishes requirements that ensure that data will be adequately protected even when processed offshore. Likewise, Model #674 can protect consumers when data is processed outside of the United States by requiring licensees to exercise oversight of offshore vendors and to enact appropriate contractual protections based on the risk of the vendor. Indeed, doing so is already a common practice within the insurance market.

*CAI Recommendation*. The requirement to obtain consumer consent prior to processing data outside the US should be deleted. Rather, the Model should rely on appropriate third-party service provider oversight obligations to require that licensees perform appropriate due diligence on all service providers, including offshore service providers. This should include a requirement to ensure that any data processed by an offshore service provider is, via contract or otherwise, subject to the oversight provisions in the Model (see discussion below in Section 5). Taking this approach would

strike an appropriate balance by protecting consumer personal information processed offshore, without disrupting current business practices.

**4. The requirement that the consumer must consent to the use of the consumer's personal information in certain actuarial studies and research activities would significantly restrict the ability of insurers to conduct necessary insurance functions.**

Section 4(E) places limits on actuarial studies and research, other than those conducted for rating and risk management purposes for the benefit of the licensee using consumers' personal information, by requiring that a licensee obtain a consumer's prior express consent before processing, retaining, or sharing a consumer's personal information in connection with actuarial studies and research. After consumer consent is obtained, Section 4(E)(1) would require that:

- No consumer can be identified in any research study or report;
- All materials allowing the consumer to be identified be returned to the licensee that initiated the study; and
- A consumer's personal information be deleted as soon as the information is no longer needed for the specific actuarial or research study.

These restrictions would provide little benefit to consumers, who are not impacted or inconvenienced by having personal information included in such actuarial studies. But it could significantly impede the ability of licensees to manage and understand their business. It is common practice for insurers to review certain aspects of their business, such as marketing. . This provision, as written, would hamper the ability of licensees to carry out important internal research and review.

No other privacy law restricts any actuarial studies and research by requiring that consumers consent to the use of their data in such studies. By preventing licensees from conducting common product and business research, Section 4(E) of Model #674 would place insurers at a competitive disadvantage when trying to understand their customers and their needs.

The CAI recognizes that any disclosure or sharing of personal information in connection with research does come with some level of increased cybersecurity risk; however, we believe those risks are appropriately addressed through existing NAIC Model Law #668.

*CAI Recommendation*. Section 4(E) should be revised to allow insurers to use and share consumers' personal data in actuarial studies and research activities for any specifiedpurpose related to insurance, subject to standard obligations for oversight of third party service providers.

**5. The requirements for enhanced third party oversight and contracting requirements would adversely limit the ability of licensees to hire top service providers.**

Section 2 of draft Model #674 would require all third parties that process data in connection with an insurance transaction to be obligated to comply with Model #674 and the licensees own privacy practices. This requirement would appear to function as a long-arm application of Model #674 that service providers would not agree to. Many service providers, such as leading cloud providers, would be unwilling to agree to be subject to compliance with every state's adopted version of Model #674, legislation that would not otherwise apply. Additionally, some service providers would already be subject to GLBA data protections adopted by the SEC or other regulators, and would be unwilling to comply with broader and more stringent insurance specific requirements under Model #674.

For example, insurance company separate accounts investing in underlying mutual funds (UIT separate accounts) necessarily interact with SEC-regulated transfer agents, funds, and investment advisors. It appears that such entities would qualify as service providers of the UIT separate account

under draft Model #674. However, such entities are regulated by the SEC and would likely be unwilling to agree to be subject to the specific requirements of Model #674. If such entities did refuse to adopt the specific contractual obligations required under the Model, the UIT separate account would then be prohibited from continuing to use these SEC-regulated entities. That would then force the UIT separate accounts to attempt to rearrange the entire structure of existing placement and administration of its investments into new and different funds, advisors, and other counterparties, rearrangements that could require SEC approval. This would cause costs and disruption to consumers, while also raising legal and regulatory risks and uncertainties around breach of contract and SEC regulatory requirements.

*CAI Recommendation*. Instead of applying a one-size-fits-all approach that will limit the ability of licensees to engage the best service providers in the market, Model #674 should be revised to take a risk-based approach. The CAI recommends that the Model require licensees to conduct appropriate due diligence and oversight of all third party service providers that process personal information, and require licensees to negotiate appropriate contractual protections based on the assessed risk of the service provider. The Model should not specify what those contractual protections would include beyond limiting the service providers ability to use, share or disclose personal information for purposes other than providing the services.

Additionally, the CAI recommends that the definition of "third party service provider" be revised to exclude affiliates of licensees, and that the Model provide an exemption for the sharing of personal information to entities already subject to Model #674 or the GLBA.

**6. Compliance with the 90-day deletion requirement will not be possible to meet in many circumstances, and the related notice requirement will likely be confusing to consumers.**

Section 5.B. of draft Model #674 requires a licensee to completely delete all of the consumer's personal information within 90 days after the data is no longer necessary to perform any of eight permitted purposes described in Section 5.A. In addition, any third party service provider must notify the licensee when the consumer's information is completely deleted.

The 90-day timeframe for deleting all of a consumer's information in the possession of the insurer is too short and not practical given the number of systems on which a consumer's data may be retained. Personal consumer information can be retained on application, underwriting, operational, claims, marketing and other systems. Some systems may be retired legacy systems that require special programming to delete consumer data, if deletion is even possible. Consumer data can also appear on backup systems that present special issues. Moreover, given the length of time that some personal data must be retained, some consumer data may be on first generation systems where institutional programming knowledge has been lost or the data may even be in paper files that are archived and very difficult to access. In short, the 90-day deadline for deleting data does not reflect the practical challenges of deleting data at an institutional level, and should be revised to take into account the complex realities of record keeping and record deletion across the industry. We also note that the cybersecurity risks associated with retention of personal information is already addressed in Model #668, which requires that a licensee's information security program "define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed."

Section 5.B also does not address whether it applies retroactively, that is, how this provision will apply to personal consumer information that has been retained for many years beyond the deadlines in this Section.

Finally, Section 5.B. (3) would require a licensee that no longer has a relationship with a consumer in connection with any insurance transactions to send a notice to the consumer that the licensee no longer retains the consumer's personal information. This notice provision is

unprecedented and would be difficult to implement. Moreover, it is likely that a consumer who no longer has a relationship with the licensee will be very confused, and possibly concerned, upon receiving such a notice.

*CAI Recommendation*. Section 5.B. should be revised to allow insurers a reasonable amount of time to delete personal data that is no longer necessary. The Model should not specify a one-size-fits all time period for doing so. Section 5.B. (3) should be deleted in its entirety.

**7. The notice requirements are too complicated and would dilute their value to consumers.**

While effective and transparent notice is an essential part of consumer privacy protections, the obligations proposed in Model #674 are too broad and would be difficult to meet in practice. The notices would also be hard to understand and not consumer friendly.

Section 6 of the draft Model would create obligations that are impossible to comply with in practice because of the broad definition of a "consumer". As proposed, the Model would require full and annual notification, prior to or at the point of collection, to not only policyholders and annuitants but also claimants, beneficiaries, agents, guardians, and other individuals who do not have a direct relationship with the licensee. In many cases, this will be an impossible standard to meet. For example, it would be impossible for a UIT separate account to provide a privacy notice to the beneficiary of a variable annuity prior to the annuitant actually providing to the UIT separate account the name and other personal information of the beneficiary. Where the licensee does not have a direct relationship with the consumer, licensees cannot know who the consumer is until it has already collected personal information about them.

Additionally, the requirement to provide annual privacy notices to all consumers, even where nothing has changed since the last notice was provided, cuts against the trend in both state law and in federal regulations to reduce the number of annual privacy notices that consumers receive. For example, the SEC is currently proposing amendments to Regulation S-P (which implements GLBA privacy and security requirements) that provides relief from having to provide annual notice where a notice has previously been provided and an entity's privacy practices have not changed. That is consistent with the FAST Act, which was adopted by Congress in 2015 and revised the GLBA annual notice requirement. It is also consistent with the NAIC's own Model Bulletin on GLBA annual privacy notices[5] published in response to the FAST Act, which similarly adopted this more streamlined approach. We suggest that more notice to consumers is not always better. Rather, if consumers receive too many and too frequent privacy notices, it reduces the usefulness and effectiveness of consumer notice in practice.

Section 7 of the draft Model would also require a range of specific disclosure obligations that would be impractical or impossible to meet, while also removing the ability of licensees to be able to use and rely on the federal Model Privacy Form. For example, Section 7.A.(4) would require licensees to identify the specific sources that may be used to collect information about a consumer. However, those sources may not be known for each consumer prior to collecting the data. Additionally, this would suggest that a licensee would be required to update its privacy notices prior to engaging a new vendor to provide consumer data in connection with providing financial products or services.

Similarly, the right under Section 7.A.(6) to obtain a list of the specific persons with which their personal information has been shared in the previous year would be difficult to comply with in practice, while providing little benefit to consumers. As drafted, this notice would be required to cover

[5] The *Gramm Leach Bliley Act Annual Privacy Notice NAIC Model Bulletin* is available at https://content.naic.org/sites/default/files/inline-files/legal_bulletin_gramm_leach_bliley_act_annual_privacy_notices.pdf

any individual, internal or external, with whom the licensee shared the information. The effort to track each internal individual who helps process requests for services associated with a consumer's annuity, or who helps process a claimant's claim, would be daunting if not impossible in practice, while the benefit to the consumer of receiving such a list is unclear. While this right is similar to an existing right under Section 8.A.(2) of Model #670, that right only applies to the extent the requested information is actually recorded, and otherwise only requires a description of the persons to whom such information is normally disclosed.

Further, for licensees like UIT separate accounts that would be subject to both Model #674 and the SEC's Regulation S-P or other implementations of the GLBA's privacy requirements, Sections 6 and 7 would also subject such licensees to inconsistent and potentially conflicting notice requirements, possibly resulting in two different privacy notices to be sent to the same individuals for the same product.

*CAI Recommendation*. The notice and disclosure requirements in draft Model #674 should be revised to more closely follow the existing notification structure and obligations under Model #672, while appropriately building on those requirements to enhance the quality and transparency of consumer notice. Licensees should also be required to publicly post their privacy notices online and make them available on request, in lieu of having to provide direct notice to individuals that would not currently qualify as customers under Model #672. The overall disclosure obligations should be generalized to allow for practical descriptions and disclosures, such as disclosing the types of sources from which personal information is collected instead of the actual sources. Finally, an updated model form should be developed that would allow licensees to meet the disclosure obligations of Model #674 while also complying with existing requirements for using the Federal Model Form. Doing so would allow licensees to continue to benefit from the safe harbors for using the Federal Model Form while also promoting broader use of consistent and consumer friendly notification practices.

**8. The optional private right of action provision should be removed.**

Section 28 of proposed Model #674 would provide an option to state legislatures to include a limited private right of action for any failure to comply with the Model that also violates an individual's rights under the Model. We appreciate that the Working Group has included limitations, such as limiting suits to actual damages and prohibiting class actions. However, this limited private right of action is still ripe for abuse and would subject licensees to litigation related expenses regardless of whether the licensee is fully compliant. Consumers also do not need a private right of action to empower them to thwart inappropriate conduct by a licensee, as consumers are able to file complaints of any violations with state regulators. Regulators already maintain robust complaint intake functions, which are well equipped to identify legitimate issues and ensure licensees appropriately address those issues. Accordingly, enforcement authority for compliance with Model #674 should rest with state regulators.

*CAI Recommendation*. Proposed Section 28 should be revised to remove the option for state legislatures to include a limited private right of action under Subsection B, and instead specify that the law does not create a private right of action using the existing language under Subsection A.

We want to express our deep appreciation for the opportunity to comment on draft Model #674, and we hope that you find these comments helpful at this stage. Please do not hesitate to contact us if you have any questions.

Sincerely,

**For The Committee of Annuity Insurers**

Eversheds Sutherland (US) LLP

By:



Stephen E. Roth
Mary Jane Wilson-Bilik
Alexander F. L. Sand
Eversheds Sutherland (US) LLP

EVERSHEDS SUTHERLAND

**From:** Roth, Stephen
**Sent:** Wednesday, July 26, 2023 1:37 PM
**To:** CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
**Cc:** Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
**Subject:** Fatal Flaw Draft CAI Comment Letter on Revised Draft of Proposed Model Law #674 - Comments by 11 am ET on 7/28
**Importance:** High

Following up on our July 20 call, during which we discussed an outline that we prepared of proposed comments on the revised draft of NAIC Proposed Model #674, we are attaching for your review and comment a draft of the comment letter that we propose to submit on behalf of the Committee of Annuity Insurers. The attached draft includes the comments we had included in that outline, as well as some additional comments, for example on the provisions dealing with joint marketing arrangements.

Given the very short comment period, and because the draft closely tracks what we discussed with you on the July 20 Working Group call, we are treating this as a fatal flaw draft. **We are asking that you provide us with any comments or edits to the draft by 11 am ET on Friday July 28** so we can incorporate any changes into the letter we plan to submit by close of business that same day. If you have any significant comments or concerns, we would greatly appreciate hearing from you *sometime tomorrow* if that is possible. (For ease of reference we are also attaching the revised exposure draft as well as the CAI comment letter on the initial exposure which we reference in certain places in the attached draft.)

We really appreciate the helpful input we received on the July 20 Working Group call. If you do have comments, suggestions or edits on the attached draft, please contact Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) or me.

Steve

**Stephen E. Roth** | Partner | T: +1.202.383.0158

**From:** Roth, Stephen
**Sent:** Tuesday, July 18, 2023 9:44 PM
**To:** CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
**Cc:** Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
**Subject:** Draft Outline of CAI Comment Letter on Revised Draft of Proposed Model Law #674; CAI Call 7/20 @ 3pm ET

Hi everyone,

Following up on our July 14 note regarding the revised draft of NAIC Proposed Model #674, we have prepared the attached discussion draft *o*utline of potential issues on which the CAI could comment that we would like to discuss on the CAI Cyber & Privacy Working Group's call this **Thursday, July 20 at 3 pm ET**. If you have an opportunity to review and consider what we have outlined before Thursday, that would be great. In any event, we will walk through the draft outline on Thursday's call so as to obtain Committee member reaction and comments.

Given the short comment period, we will be looking for direction from the Working Group on Thursday whether to proceed with preparing a draft comment along the lines outlined, subject to further thoughts Working Group members may have.

EVERSHEDS SUTHERLAND

We are sending out a calendar invite for Thursday's Zoom meeting. In the meantime, if you have questions or comments, please don't hesitate to contact Mary Jane (202-383-0660), Al Sand (512-721-2721) or me.

Steve

**From:** Roth, Stephen
**Sent:** Friday, July 14, 2023 1:18 PM
**To:** CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
**Cc:** Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
**Subject:** NAIC Privacy Protection (H) Working Group Releases Revised Draft of Proposed Model Law #674; CAI Call 7/20 @ 3pm ET

On July 11, the NAIC's Privacy Protection (H) Working Group (the "Working Group") released a revised draft of Proposed Model Law #674 (Insurance Consumer Privacy Protection Model Law) (the "Revised Proposal"). This Revised Proposal (attached) makes significant substantive revisions to the previous proposal, and follows significant industry feedback on the initial proposed draft, including the comment letter we submitted on behalf of the Committee on April 3, 2023 (attached) and our appearance on behalf of the Committee during in-person meetings in Kansas City on June 5 and 6, 2023. **Comments on the Revised Proposal are due by Friday July 28.**

Based on our initial review of the Revised Proposal, the Working Group appears to have taken a more favorable approach on many of the issues that the Committee and other interested parties were concerned about, including:

- moving toward an opt-out (instead of consent/opt-in) regime for marketing
- specifically permitting joint marketing
- establishing more flexible privacy notice requirements
- providing more flexibility on data retention and destruction

However, the Revised Proposal still includes items of concern that will likely warrant further comment from the Committee, including:

- Requiring consent to collect, process or share consumer personal information in connection with "additional activities" (an undefined term)
- Limiting the definition of an "insurance transaction" for which personal information may be processed to an enumerated list of authorized activity
- Unclear and confusing drafting around opt-out vs. opt-in requirements, including possibly conflating whether some sort of authorization is required for marketing
- Requiring licensees who use legacy systems that do not allow the deletion of personal information to migrate to new systems within 10 years unless otherwise approved by state insurance regulators.

For your reference, attached is a redline of the Revised Proposal against the previously proposed version. We are continuing to review the Revised Proposal to identify areas of concern for potential comment.

**We will hold a call on Thursday, July 20 at 3pm ET/2pm CT** of the Committee's Cyber & Privacy Working Group to discuss the Revised Proposal. The information for that call is as follows:

EVERSHEDS SUTHERLAND

**DATE AND TIME: Thursday, July 20 @ 3 pm ET**

| | |
|---|---|
| **Join By Telephone** | |
| **Dial In:** | +1 646 558 8656 |
| **Meeting ID:** | 5787221869 |
| **Pass Code:** | 339516 |
| | |
| **Join Web-Based Meeting** | **Join Zoom Meeting** |
| **One-Tap Mobile:** | +16465588656,,5787221869#,,,,*339516# |
| **Meeting URL:** | https://eversheds-sutherland-us.zoom.us/j/5787221869?pwd=K1FoZTRweG0ybFVoUnZCVHd1WUczdz09 |

Given the very short comment period, our gameplan at this juncture is to:

- circulate an *outline of a proposed CAI comment letter* in advance of the July 20 call that we can walk through during the call so we can hear Committee member feedback, comments and concerns; and
- circulate a *draft of the CAI comment letter* on Tuesday July 24 for Committee member review and comment. Our hope is to be able to reflect any comments in the final CAI comment letter we would submit on Friday, July 28. If necessary, however, we will circulate a fatal flaw draft and/or hold a call to discuss any significant Committee member concerns with the draft.

If you have any comments or thoughts in the meantime, please send them to me, Al Sand, or MJ. We appreciate the ongoing opportunity to work with you all on these important issues.

Steve

**From:** Roth, Stephen
**Sent:** Thursday, June 15, 2023 2:32 PM
**To:** CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>
**Cc:** Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>
**Subject:** Update on NAIC Privacy Protection (H) Working Group's Continued Work on Proposed Model Law #674

We are writing to provide an update on the NAIC's Privacy Protection (H) Working Group's (the "Working Group") continued work on Proposed Model Law #674 (Insurance Consumer Privacy Protection Model Law) and our ongoing efforts to engage with the Working Group on behalf of the Committee.

Executive Summary. Following up on the comment letter we submitted on behalf of the Committee of Annuity Insurers on April 3, 2023 (attached), we appeared on behalf of the Committee before the Working Group on June 5 and 6 during a two-day in person working session to express the Committee's concerns and requests for changes to the current proposed draft of Model #674. Specifically, Al Sand attended the two day session in Kansas City and expressed concerns consistent with those set forth in the Committee's comment letter. Following the working session, the Working Group plans to significantly revise the proposed model and expose a new version for comment by July 4, 2023. The Working Group

continues to plan to finalize a proposed Model # 674 to send to the Innovation, Cybersecurity, and Technology (H) Committee during the 2023 Fall Annual Meeting in late November.

Report on June 5 & 6 Two-Day Meeting. On June 5 and 6, 2023, the Working Group held a two-day in person working session in Kansas City, Missouri to work through several of the most contentious issues raised by the current draft of Model #674. The topics discussed by the Working group, industry groups, and consumer representatives during the two days were:

- Data minimization requirements and limitations on the purposes for which insurance licensees may collect and use consumer personal information;
- Consent requirements to be able to market to consumers, including existing customers;
- Joint marketing;
- Third-party service provider oversight and contracting requirements; and
- The content and frequency of consumer privacy notices.

Over the two-day event, Al participated in each discussion session to comment on behalf of the Committee consistent with the positions set forth in the Committees' April 3, 2023 comment letter. This included emphasizing the following points:

- Limitations on the ability to market insurance products would create an uneven playing field that would disadvantage annuity products competing with other non-insurance investment products;
- Consent requirements for marketing would effectively prohibit joint marketing with trusted financial institution partners and inhibit the ability to inform the market about annuities and other beneficial financial products;
- Narrow limitations on the purposes for which personal information can be collected and used would inhibit insurers from engaging in non-insurance activities, as well as their ability to innovate;
- Proposed third-party service provider oversight and contracting requirements would limit the ability of Committee members to choose the best vendor for their needs; and
- Overly specific and frequent notice requirements would be impossible to satisfy in practice while also reducing the effectiveness of the notices.

Industry groups expressed universal concern and opposition to the current draft of Model #674 during the discussion periods, frequently expressing concerns similar to those highlighted on behalf of the Committee. The Chair of the Working Group, Katie Johnson from Virginia, acknowledged from the beginning of the two-day session that the Working Group expected significant revisions were needed to the proposed model and that they appreciated and valued the feedback provided.

The Working Group, in particular a few vocal members of the Working Group from Maine, California, and North Dakota, expressed a wide range of concerns that they were interested in addressing through the new Model Law, including:

- Empowering consumers with control of the purposes for which their data may be collected and used, such as being marketed to;
- Providing meaningful and transparent notice to consumers to empower them to exercise choice within the market based on privacy practices and take steps to protect their personal information;
- Addressing cybersecurity risks above and beyond what is currently in existing Model #668 (Insurance Data Security Model Law); and
- Concern over licensees engaging in, and leveraging consumer personal information for, inappropriate non-insurance activities.

At the conclusion of the two-day working session, and after a regulator-only session to discuss next steps, the Working Group announced that it planned to draft a significantly revised version

of the proposed model by July 4 with the intent of addressing many of the comments received. Comments from Chair Katie Johnson appeared to indicate that the revised draft will move to a more opt-out-focused (instead of consent-focused) regime, and would provide allowances for joint marketing. The Working Group continues to plan to finalize a proposed Model # 674 to send to the NAIC's Innovation, Cybersecurity, and Technology (H) Committee by the 2023 Fall Annual Meeting in late November.

If you have any questions about this report or the status of draft Model #674, please contact Al Sand, Mary Jane Wilson-Bilik or me. We will continue to monitor and report on developments emanating from the Working Group.

Steve

**From:** Roth, Stephen
**Sent:** Wednesday, April 12, 2023 11:20 AM
**To:** Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>
**Cc:** CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
**Subject:** Final CAI Comment Letter on NAIC Proposed New Privacy Model Law #674

Last week we submitted the attached comment letter on behalf of the Committee of Annuity Insurers to the NAIC on its draft proposed new privacy model law, #674. The final letter reflects the input and many helpful comments we received from Committee members over the past several weeks as we worked to develop the comment letter.

In terms of next steps, at the NAIC Spring National Meeting, the Privacy Protections (H) Working Group met to discuss the draft. At the outset of that meeting, Chair Katie Johnson (VA) reiterated that the exposure draft was an "initial" version of the draft that was intended to "put a stake in the ground" and encourage interested stakeholders to come to the table. Chair Johnson noted that the Working Group will continue to hold one-on-one discussions with interested parties and that it expects to hold biweekly virtual listening sessions (beginning April 18) and at least one in-person meeting (to be held in Kansas City, Missouri, June 4-6) to further refine the draft model. The Working Group currently expects to finalize the Model Act in November 2023.

We will be closely monitoring developments relating to Model #674, will be reporting to the CAI's Cyber & Privacy Working Group in that regard, and will seek input from CAI Cyber & Privacy Working Group members on how the CAI can most helpfully continue to advocate for a workable model law.

*If you are not on the roster for the CAI's Cyber & Privacy Working Group and would like to join the Working Group*, please click here.

Steve

EVERSHEDS SUTHERLAND

**From:** Roth, Stephen
**Sent:** Friday, March 31, 2023 11:36 PM
**To:** Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>
**Cc:** CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
**Subject:** FATAL FLAW REVIEW: CAI Comment Letter on NAIC Proposed New Privacy Model Law #674

Following up on our March 30 conference call, we are attaching both clean and marked versions of a revised draft of the CAI's comment letter on the NAIC's proposed new privacy model law, Model #674. This revised draft reflects comments we received on the initial draft both before and during yesterday's call of the CAI's Cyber & Privacy Working Group. **WE ARE REQUESTING ANY FINAL FATAL FLAW COMMENTS OR EDITS TO THE LETTER BY MONDAY, APRIL 3 @ 1 PM ET** so that we can submit the letter to the NAIC by close of business Monday.

The revised letter reflects a number of changes and refinements. Most notably, an eighth section has been added advocating that the optional provision in the exposed draft providing for a private right of action be removed. In addition, a number of edits have been made throughout to modify the tone of the letter given the dialogue that industry representatives had with regulators at the NAIC Spring National Meeting, and regulator acknowledgement that the exposed draft is "initial" version of the model law and that there will be listening sessions and opportunity for further dialogue and stakeholder input over the next several months. Other changes have been made to better emphasize key issues identified by member companies.

We very much appreciate the very helpful Committee member input we have received on the letter. If you do have any final comments, please contact Mary Jane Wilson-Bilik (202-383-0660), Al Sand (512-721-7127) or me.

Steve

**Stephen E. Roth** | Partner | T: +1.202.383.0158

**From:** Roth, Stephen
**Sent:** Saturday, March 25, 2023 9:15 PM
**To:** Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>
**Cc:** CAI-Cyber & Privacy Working Group <CAI-Cyber&PrivacyWorkingGroup@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <MJWilson-Bilik@eversheds-sutherland.us>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
**Subject:** Draft CAI Comment Letter on NAIC Proposed New Privacy Model Law #674 - March 30 CAI Call

In response to our March 13 note, below, we heard from a number of Committee members who indicated that they would support a CAI comment letter on the NAIC's draft new privacy model law, Model #674. We did not hear from anyone to the contrary. We therefore have undertaken to prepare a draft of a comment letter and are attaching it here for your review and comment.

In preparing the attached draft, we focused on those issues we identified in our prior correspondence below, and that we discussed during the well-attended call we held on March 13.

Please provide any comments, suggestions or edits to the draft by **Thursday, March 30** to me, Mary Jane Wilson-Bilik (202)-383-0660 or Al Sand (512-721-2721), both of whom are also copied above. The comment deadline is Monday, April 3.

EVERSHEDS SUTHERLAND

***We also are scheduling a call of the Committee's Cyber & Privacy Working Group on <u>Thursday, March 30 at 11 am ET</u> to discuss and walk through the draft comment letter and to take any comments and suggestions that you would like to share during that call. Everyone is welcome to attend, but please let us know if you are interested in joining the CAI Cyber & Privacy Working Group.***

The information for the March 30th call is as follows:

**DATE AND TIME: Thursday, March 30 @ 11 am ET**

| | |
|---|---|
| **Join By Telephone** | |
| **Dial In:** | +1 646 558 8656 |
| **Meeting ID:** | 5787221869 |
| **Pass Code:** | 339516 |
| | |
| **Join Web-Based Meeting** | **<u>Join Zoom Meeting</u>** |
| **One-Tap Mobile:** | <u>+16465588656,,5787221869#,,,,*339516#</u> |
| **Meeting URL:** | <u>https://eversheds-sutherland-us.zoom.us/j/5787221869?pwd=K1FoZTRweG0ybFVoUnZCVHd1WUczdz09</u> |

Enjoy the rest of the week-end.

Regards,

Steve

**Stephen E. Roth** | Partner | T: +1.202.383.0158

**From:** Roth, Stephen
**Sent:** Monday, March 13, 2023 6:49 PM
**To:** Committee of Annuity Insurers <<u>CommitteeofAnnuityInsurers@eversheds-sutherland.us</u>>
**Cc:** CAI - Cyber Working Group <<u>CAI-CyberWorkingGroup@eversheds-sutherland.us</u>>; <u>mjwilson-bilik@eversheds-sutherland.com</u>; Sand, Alexander <<u>AlexanderF.L.Sand@eversheds-sutherland.us</u>>; <u>maureenadolf@eversheds-sutherland.com</u>
**Subject:** REQUEST FOR INPUT: CAI Comment Letter on NAIC Proposed New Privacy Model Law

Hello everyone,

We had a very well attended Committee of Annuity Insurers call this afternoon to discuss the NAIC's proposed new privacy model law, Model #674. During the call, we discussed the key elements of the proposed model law that we identified in our February 22 note (below) as significant changes in the NAIC model law framework, as well as the revised disclosure/notification obligations. We highlighted problematic aspects of these elements from a practical and operational perspective, including some that would be particular to variable annuity issuers.

During today's call, we did hear from some Committee member representatives that they believed it would be helpful for the Committee to prepare and submit a comment letter on proposed #674. We would appreciate hearing from additional Committee members whether you would support the Committee preparing a CAI comment letter. **If you can reply to Mary Jane Wilson-Bilik (<u>mjwilson-bilik@eversheds-sutherland.com</u> or 202-383-0660), Al Sand (<u>AlexanderF.L.Sand@eversheds-sutherland.us</u> or 512-721-2721) or me by this**

EVERSHEDS SUTHERLAND

**Thursday morning whether your company would support our engaging on this on behalf of the CAI, or whether you have any concerns with Committee submitting a comment letter, that would be very helpful.**

Assuming we do proceed with a CAI comment letter, we will target sending a draft to the Committee for review before the end of next week, and will schedule a Committee call to discuss and receive comments on the draft.

Thanks very much.

Steve

**Stephen E. Roth** | Partner | T: +1.202.383.0158

**From:** Roth, Stephen
**Sent:** Friday, March 10, 2023 10:57 AM
**To:** Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>
**Cc:** CAI - Cyber Working Group <CAI-CyberWorkingGroup@eversheds-sutherland.us>; mjwilson-bilik@eversheds-sutherland.com; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; maureenadolf@eversheds-sutherland.com
**Subject:** REMINDER: CAI Call on NAIC Proposed New Privacy Model Law for Comment - Monday, March 13 @ 2pm ET

Hello everyone,

This is just a reminder regarding Monday's call regarding the NAIC's proposed new privacy model law (#674). The ZOOM/dial-in information for the call is set forth below.

Have a good week-end.

Steve

Stephen E. Roth | Partner | T: +1.202.383.0158

**From:** Roth, Stephen
**Sent:** Monday, March 6, 2023 9:07 AM
**To:** Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>
**Cc:** CAI - Cyber Working Group <CAI-CyberWorkingGroup@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Adolf, Maureen <MaureenAdolf@eversheds-sutherland.us>
**Subject:** CAI Call on NAIC Proposed New Privacy Model Law for Comment - Monday, March 13 @ 2pm ET

We are following up on our February 22nd note, below, regarding the NAIC's exposure of its new model privacy law, Model #674. We have heard from a number of Committee members that it would be helpful to schedule a Committee of Annuity Insurers call to discuss the proposal and the issues it would raise for Committee members. We therefore are scheduling a call for that purpose on Monday, March 13 at 2 pm ET. The information for the call is as follows:

EVERSHEDS SUTHERLAND

**DATE AND TIME:** **Monday, March 13 @ 2 pm ET**

| | |
|---|---|
| **Join By Telephone** | |
| **Dial In:** | +1 646 558 8656 |
| **Meeting ID:** | 5787221869 |
| **Pass Code:** | 339516 |
| | |
| **Join Web-Based Meeting** | **Join Zoom Meeting** |
| **One-Tap Mobile:** | +16465588656,,5787221869#,,,,*339516# |
| **Meeting URL:** | https://eversheds-sutherland-us.zoom.us/j/5787221869?pwd=K1FoZTRweG0ybFVoUnZCVHd1WUczdz09 |

In addition to discussing the various elements of proposed Model #674 and related issues/concerns, we will be interested in hearing from Committee members whether a Committee comment letter focusing on specific aspects of the proposal and/or supporting other industry trade comment letters would be helpful.

If you have thoughts or comments you would like to share before the March 13th call, please reach out to Mary Jane Wilson-Bilik (202-383-0660), Al Sand (512-721-2721) or me.

Steve

Stephen E. Roth | Partner | T: +1.202.383.0158

**From:** Roth, Stephen
**Sent:** Wednesday, February 22, 2023 9:26 AM
**To:** Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>
**Cc:** CAI - Cyber Working Group <CAI-CyberWorkingGroup@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>; Adolf, Maureen <MaureenAdolf@eversheds-sutherland.us>
**Subject:** NAIC Exposes Proposed New Privacy Model Law for Comment - MEMBER INPUT REQUESTED

As you may have heard, earlier this month, the NAIC Privacy Protections (H) Working Group exposed a new model privacy law, Model #674, for comment. Model #674 would replace Models #670 and #672, which have been the cornerstones of insurers' and all insurance licensees' privacy programs for more than twenty years. The proposed Model #674 would be even more stringent than California's CCPA in many respects, substantially limiting insurers' ability to use consumer personal data and expanding privacy rights and protections for consumers.

In the five states that have adopted new comprehensive privacy laws, such as California, insurers are either completely or mostly exempt from complying with the new laws because of the laws' exemption for data or entities that are subject to the Gramm-Leach-Bliley Act (GLBA), embodied in Model #672. This means that proposed Model #674 would be a heavy lift for just about all Committee members.

Among the significant changes proposed in Model #674 are:

EVERSHEDS SUTHERLAND

1. A requirement that licensees obtain a consumer's consent before using the consumer's personal information to market a product or service to the consumer, even if the consumer is an existing customer;
2. A prohibition on using sensitive personal information for marketing and on selling personal information even if the consumer consents, except where permitting under the Fair Credit Reporting Act;
3. A prohibition on collecting or processing personal information outside the United States without the consumer's consent, severely limiting an insurer's ability to use offshore service providers;
4. A requirement that the consumer must consent to the use of the consumer's personal information in actuarial studies, research and other permitted transactions; and
5. A requirement for enhanced third party oversight and contracting requirements.
6. A requirement for licensees to securely delete consumer personal information if it is no longer necessary to perform specific "permitted purposes" after 90 days.

Proposed Model #674 would also strengthen existing consumer rights, including mandating a more detailed privacy notice and tightening obligations around a consumer's right to access and correct personal information. Proposed Model #674 would give state legislators the option to include a private right of action when they enact the model into law.

***For a more detailed summary of proposed Model #674, see the Eversheds Sutherland Legal Alert***: ES Model #674 Alert .

Comments on proposed Model #674 are due to the NAIC by April 3, 2023. ***We are interested in whether Committee members believe it would be useful and informative to schedule a Committee call to discuss proposed Model #674 and its implications, and/or whether Committee members believe that a Committee comment letter to the NAIC on the proposal would be helpful from an overall industry comment perspective. Please let us know if you believe we should schedule a Committee call to discuss the proposal and a possible comment letter.***

Please reach out to Mary Jane Wilson-Bilik (202-383-0660), Al Sand (512-721-2721) or me if you have questions and to share your thoughts regarding whether you believe further CAI engagement would be helpful.

Steve