EVERSHEDS SUTHERLAND

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

August 14, 2023

VIA E-Mail
Joanne Berman
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: **Comments on Revised Proposed Second Amendment to 23 NYCRR 500**

Dear Ms. Berman:

This comment letter is submitted on behalf of the Committee of Annuity Insurers (the "Committee").[1] The Committee is pleased to have the opportunity to offer its comments on the New York State Department of Financial Services' (the "Department") Revised Proposed 2nd Amendment to Regulation 23 NYCRR Part 500 (June 28, 2023) (the "Revised Proposal").

The Committee appreciates that the Revised Proposal includes numerous revisions that respond to and address concerns raised by the Committee in its previous comment letter and by others. The Committee views the Revised Proposal as a significantly improved and more pragmatic approach compared to the previous version of the proposal. We also appreciate the thorough Assessment of Comments provided by the Department and the transparency it provides on the Department's views on these important issues.

That said, the Committee continues to stand by the comments and suggestions we raised in our previous letter that have not been adopted by the Department. However, while the Committee continues to believe that its comments that were not adopted should be addressed, this comment letter does not revisit those issues that have been fully considered by the Department in the Assessment of Comments. The comments set forth herein reflect Committee members' consideration of the Revised Proposal and relate to several new or remaining issues that we believe the Department has not yet fully considered. Further, it is our belief that the Department can address these issues without making substantive changes to the existing Revised Proposal such that an additional comment period would be required.

[1] The Committee is a coalition of many of the largest and most prominent issuers of annuity contracts. The Committee's current 32 member companies represent approximately 80% of the annuity business in the United States. The Committee was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of insurance, securities, banking, and tax policies regarding annuities. For over four decades, the Committee has played a prominent role in shaping government and regulatory policies with respect to annuities at both the federal and state levels, working with and advocating before the SEC, CFTC, FINRA, IRS, Treasury Department, and Department of Labor, as well as the Department and the relevant NAIC and Congressional committees. A list of the Committee's member companies is available on the Committee's website at www.annuity-insurers.org/about-the-committee/.

Eversheds Sutherland (US) LLP is part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, please visit www.eversheds-sutherland.com.

1. The Proposed Requirement That the Board Annually Approve the Cybersecurity Policy is Overly Prescriptive and Unnecessary

The Committee recognizes that the Revised Proposal has been revised to at least partially address concerns raised by the Committee that the requirements would conflate the roles of the Board and Management.

That said, the Committee continues to believe that the proposed requirement for the Board (or Senior Governing Body) to annually approve the covered entity's cybersecurity policy is overly prescriptive, conflates the roles of management and the Board, and is ultimately unnecessary to achieve the Department's goals. We agree with the Department's statement in its Assessment of Comments that "[t]o properly exercise oversight responsibility, the board or other senior governing body must be aware of cybersecurity risks and ensure the company has a written cybersecurity policy and procedures in place." However, requiring the Board to annually approve the cybersecurity policy itself is not required to meet this goal, and is largely a form over function approach.

In responding to commenters, the Department argues that this requirement is not overly burdensome because it does not require the Board to approve procedures containing overly specific or technical details, rather only the higher-level policy. This statement itself illustrates that this requirement is taking an overly prescriptive form-focused approach instead of a principles-based approach. In practice, there is no one standard for how much technical information is contained in a policy compared to what is separated out into separate procedures or guidance documents. There is an incredible variety in the content, form, and thoroughness of documents that are deemed "policies" within an organization. In some cases, a policy document could contain insufficient information to be useful to the Board in exercising its oversight obligations. In others, the existing policy documentation may contain entirely too much information to be useful to the Board, and so the covered entitiy would need to revise and redefine all of its "policies" simply to enable functional engagement with the Board. Doing so would be a non-substantive exercise that would entail a significant investment of time and resources in order to enable compliance with the letter of the Revised Proposal's requirements.

Rather, the Committee suggests that the goal of the Department to ensure that Boards exercise appropriate oversight over the cybersecurity risks of a covered entity are already adequately addressed by the requirement under Section 500.04(d)(1) to exercise "effective oversight of the covered entity's cybersecurity risk management . . . ." If the Department wishes to emphasize that oversight should include appropriate review and understanding of the covered entity's cybersecurity policies, we believe that would be best accomplished through the use of guidance. Alternatively, this point could be clarified by deleting the annual approval language from 500.3 and adding a phrase to the end of 500.04(d)(1) stating that oversight should include assessment of the covered entity's cybersecurity policies. Requiring Boards to approve a cybersecurity policy document does little in practice to ensure that Boards are exercising effective oversight, while creating unnecessary and burdensome compliance hoops for the Board and the covered entity.

2. The Revised Definition of a "Violation" Continues to be Overly Broad and Problematic

Section 500.20 of the Revised Proposal establishes a new definition for what constitutes a "violation" of Part 500. Although the addition of a materiality standard to Section 500.20(b)(2) is helpful, Section 500.20(b)(1) continues to be overly broad and problematic.

This section would define a violation to include the failure to "prevent unauthorized access to an individual's or entity's nonpublic information due to noncompliance with any section of this Part." Including the occurrence of a data breach as a specified example of when a violation of Part 500 has occurred is inappropriate and, at best, creates a functional presumption of a violation upon any occurrence of a data breach. The nature of cybersecurity is that while cybersecurity programs are designed prospectively to try to minimize the risk of a data breach, data breaches are an inevitable occurrence. Breaches are perpetrated by malicious bad actors, and no organization can hope to be completely impenetrable over time. Accordingly, defining a violation to include a failure to prevent a data breach would in practice codify a retroactive and "hindsight is 20/20" approach to assessing the sufficiency of a covered entity's cybersecurity program. The covered entity will never have the benefit of

having experienced and learned from the breach when designing its cybersecurity program and policies to comply with the requirements of Part 500. Only the Department will ever have the knowledge or awareness of a breach and how the breach occurred in assessing whether the covered entity's cybersecurity program is compliant with Part 500. In this way, defining a violation to include the occurrence of a breach would unavoidably create an inappropriate bias toward determining that a breached covered entity's cybersecurity program was insufficient and non-compliant.

In the Department's Assessment of Comments, it responded to commenters concerns about this provision by noting that "a violation is not based solely on whether a breach occurred but also on whether the breach occurred because of a failure to comply with any of the requirements contained in Part 500." However, this argument is circular and tautological. The Department appears to try to differentiate between a "violation" and a "failure to comply" with Part 500, but this is a distinction without a difference. Section 500.20(b), by its own terms, defines what acts or failures constitute a violation of Part 500. These defined violations of Part 500 necessarily also constitute acts or failures that would constitute a failure to comply with some aspect of Part 500, since they are *per se* violations of Part 500. Section 500.20(b) specifically includes the failure to "prevent unauthorized access to an individual's or entities nonpublic information due to noncompliance with any section of this Part" as one of those violations. So, we do not believe that it is possible to distinguish between something that is a "violation" and something that is a "failure to comply" based on the circular language included in Section 500.20(b) of the Revised Proposal. The Department's response also misses the broader point that defining a violation by referencing a breach necessarily makes the occurrence of a breach carried out by a bad actor to be a factor in whether the covered entity itself has complied with Part 500. If a breach in of itself is not a violation of Part 500, then there is no need to reference the occurrence of a breach in defining what constitutes a violation.

Accordingly, the Committee believes that **Section 500.20(b)(1)** is inappropriate, overbroad, and unclear. This section should be deleted or revised to clarify that a violation is based solely on non-compliance with the requirements of Part 500, not whether a breach has occurred regardless of a covered entity's good faith efforts to enact a compliant cybersecurity program.

3. New Cybersecurity Event Notice Requirements Need Refinement

The Committee recognizes and appreciates that the Revised Proposal includes changes to address concerns about the breadth of the new cybersecurity event notice requirements previously raised by the Committee and others. While these revisions are helpful, they continue to need further refinement.

Section 500.17(a)(1)(iii) of the Revised Proposal would continue to require covered entities to notify the Department of any cybersecurity incident that involves the compromise of a privileged account, regardless of the nature or materiality of the compromise. We previously noted that this requirement would be overly broad, and would require over-reporting of incidents to the Department of little utility. In its Assessment of Comments, the Department recognized concerns that this notice requirement was overbroad, and sought to address the issue by removing paragraph (2) of the definition of "privileged account" so that "only unauthorized access to accounts that perform security-relevant functions that ordinary users are not authorized to perform are reportable events." While this revision is a helpful improvement, it does not fully address the issue. Further, the addition of the reference to affiliates and service providers in Section 500.17(a)(1) has created additional new issues.

As drafted in the Revised Proposal, any compromise of a privileged account would trigger the requirement to notify the Department regardless of the materiality or impact of that compromise to the covered entity. This would include any compromise of a privileged account at an affiliate or third party service provider, even if the compromise of that account has no effect on the covered entity whatsoever. The mere fact of a compromise of a privileged account is all that is required. We assume this is not the Department's intent, as the other triggers for an event notice are specifically tied back to the event's effect on the covered entity. Section 500.17(a)(1)(ii) of the Revised Proposal requires notice where the incident would have a material effect on the "operations of the covered entity." Likewise, Section 500.17(a)(1)(iv) only requires notice of ransomware within a material part of "the covered entity's information systems." No such nexus to the actual covered entity or degree of harm is currently required

for a compromise of a privileged account. This would result in significant over-reporting to the Department that would serve no purpose.

Accordingly, the Committee requests that **Section 500.17(a)(1)(iii)** of the Revised Proposal be revised to clarify that notification is only required where there is a compromise of one of the covered entity's privileged accounts and where the compromise results in a more than de minimis risk to nonpublic information or the covered entity's information systems.

Similarly, the revisions to **Section 500.17(a)(1)** requiring notice of cybersecurity events occurring at affiliates and third party service providers also appear to create unintended changes to **Section 500.17(a)(1)(i)**. As drafted in the Revised Proposal, if an affiliate or third party service provider is required to provide notice of any cybersecurity event to a governmental body, the covered entity itself would then be required to notify the Department. This would be required even if the covered entity itself has no other reporting obligations. This does not appear to be an intentional change, and would serve little practical purpose while also putting covered entities in the untenable position of having to evaluate whether a third party may have a reporting obligation around a cybersecurity event.

Accordingly, **Section 500.17(a)(1)(i)** should be revised to clarify that notification under this provision is only required when the covered entity itself is otherwise required to provide notice of the event to a supervisory body.

4. Clarify Certification of Compliance Requirements

The Committee appreciates the revisions made to Sections 500.17(b)(1) and 500.20(b)(2) to focus on material compliance instead of "full compliance." We note that **Section 500.17(b)(1)(ii)(a)** continues to refer to "full compliance" instead of "material compliance." We assume this is an unintentional oversight. **Section 500.17(b)(1)(ii)(a)** should be revised to clarify that the required acknowledgement should state the covered entity did not "materially comply" instead of "fully comply."

Additionally, as revised **Section 500.20(b)(2)** now defines a "violation" to include any failure to materially comply with any section of Part 500 for any 24-hour period. Paired with **Section 500.17(b)**, the Revised Proposal would appear to require a covered entity to file an acknowledgement of non-compliance any time the entity identifies material non-compliance over any 24-hour period. In practice, this approach inappropriately characterizes the covered entity by its worst 24-hour period. Even where an incident of non-compliance is quickly and fully remediated and the covered entity is fully compliant for most of the year and at the time of certification, the covered entitiy would still be required to file an acknowledgement of non-compliance. This will result in a large number of acknowledgements of non-compliance being filed covering incidents that are fully remediated and will serve little regulatory or risk-reduction purpose.

We therefore request that **Section 500.17 (b)** be clarified to only require covered entities to submit an acknowledgement of non-compliance if the covered entitiy is materially non-compliant as of year-end of the year that would be covered by the acknowledgement of non-compliance. Doing so would create a strong incentive for covered entities to identify and remediate compliance issues quickly, while reducing the over reporting of brief occurrences of non-compliance.

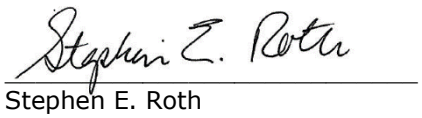
The Committee appreciates the time and resources that the Department and its staff have devoted to this Revised Proposal, as well as the opportunity to provide the Committee's views. We also appreciate the Department's careful consideration of the comments expressed herein. The Committee and its members stand ready to provide the Department with any information that may further your consideration of the concerns we have expressed and to engage in positive dialogue with the Department on these matters at your convenience.

Respectfully submitted,

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