EVERSHEDS SUTHERLAND

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

June 5, 2023

VIA E-Mail
Rule-comments@sec.gov

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: **Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information**
Release Nos. 34-97141; IA-6262; IC-34854; File Number S7-05-23

Dear Ms. Countryman:

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 in response to the request of the Securities and Exchange Commission (the "Commission") in Release Nos. 34-97141; IA-6262; IC-34854 (April 6, 2023) (the "S-P Proposing Release") for comments on proposed amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (Reg. S-P).

Committee members applaud the Commission's goal of strengthening the cybersecurity safeguards of customer information. In the S-P Proposing Release the Commission asks for comments on many aspects of the proposed amendments in order to obtain broad input on the potential impacts of and alternatives to what the Commission has proposed. The comments in this letter reflect Committee members' considered views on a number of the Commission's

[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 NAIC and relevant 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/.
.

requests for comment, so that the amendments as ultimately adopted can be effectively and efficiently implemented by individual Committee members and their various affiliated SEC-regulated entities that qualify as covered institutions under Reg S-P.

An overarching request of the Committee is for the Commission to harmonize and reconcile the considerable overlap and conflicts among the S-P Proposing Release and the other proposed and existing cybersecurity rules impacting the variable products industry. While the Commission's narrative discusses the overlap in the proposals, it does not provide clear guidance on how the industry should navigate the varying, and at time conflicting, terms and processes of the different rules and proposals. We address some of these concerns in particularity below.

1. **Clarify that complying with the incident response program requirements under proposed Rule 38a-2 of the Investment Company Act of 1940 (IC Act) would also satisfy the new incident response policy and procedure requirements set forth in the S-P Proposing Release.**

As an example of the need to harmonize the S-P Proposing Release and the other cybersecurity proposals and rules, the Committee requests that the Commission clarify that the new requirements to develop, implement and maintain written policies and procedures addressing incident response plans to detect, respond to, and recover from unauthorized access to or use of customer information under proposed Rule 30(b)(3) of Reg. S-P would be satisfied by policies and procedures meeting the requirements for cybersecurity incident response and recovery policies and procedures under proposed Rule 38a-2 of the IC Act. Committee members' registered separate accounts will be subject to both proposed rules that would establish new requirements for cybersecurity incident response policies and procedures using slightly different language for the same concept. However, neither of these proposed rules currently addresses the extent to which they are intended to overlap, be equivalent, or somehow differ. While the Committee recognizes that the proposed Rule 30(b)(3) of Reg. S-P includes specific notice requirements that are not specifically addressed in proposed Rule 38a-2, the other requirements to develop, implement, and maintain incident response policies and procedures in proposed Rule 30(b)(3) appear to be duplicative of the requirements in proposed Rule 38a-2(b)(1)(v).[2]

The Committee requests that, at a minimum, the Commission add language to the release adopting proposed Rule 30(b)(3) under Reg. S-P clarifying that compliance with the cybersecurity policy and procedure requirements under proposed Rule 38a-2(b)(1)(v) of the IC Act would satisfy the requirements of proposed Rule 30(b)(3), with the exception of the notice requirement in proposed rule 30(b)(3)(iii), which is discussed later in this comment letter.

The Committee also notes that the requirement to maintain policies and procedures to safeguard customer information under proposed Rule 30 does not currently acknowledge that those policies and procedures should be based on the specific risks of the particular covered institution and be commensurate with the size and complexity of the covered institution's activities. The Committee requests that language be added to Rule 30(b) noting that the required policies and procedures should be based on the specific risks of the particular covered institution and commensurate with the size and complexity of the covered institution's activities.

[2] See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release Nos. 33-11028; 34-94197; IA-5956; IC-34497; File No. S7-04-22) (February 9, 2022) (the "IM Cybersecurity Release") at 196-97.

2. Adjust the notice obligations in proposed Rule 30 of Reg. S-P to reflect the practical realities of responding to security incidents.

i. Allow for a reasonable determination by the covered institution of the data that was reasonably likely to have been affected by the unauthorized access when determining who must be notified of the unauthorized access or use.

Proposed Rule 30(b)(4)(ii) of Reg. S-P would require that if a covered institution cannot determine specifically which individuals' sensitive personal information was affected by an unauthorized access or use, then the covered institution must provide notice of unauthorized access to all individuals whose sensitive customer information resides in the customer information system that might have been accessed. As drafted, this requirement would create a binary and artificial approach to individual notification that would result in the over-notification of individuals on the basis of their data being stored on a certain system, regardless of whether an investigation indicates that those individuals' information may have been subject to unauthorized access.

In responding to security incidents, it is rare to have complete visibility into the acts and movements of threat actors, particularly since threat actors actively attempt to evade monitoring and to cover up evidence of their activity. Accordingly, while an investigation may be able to determine with a degree of confidence what the threat actors did and what was likely affected, in most cases covered institutions will not be able to determine exactly which individuals' information was affected and which was not within the 30 day time frame allowed in the proposed rule. Notice currently is given to individuals whose information is reasonably believed to have potentially been affected after the findings of the investigation are determined. The Committee believes this current practice is an appropriate and common-sense approach to notification.

In contrast to this common-sense approach, if the covered institution cannot determine specifically who was affected (as will often be the case), then the Proposing Release would require notice to be given to anyone whose information happens to be on the affected system, not those whose information actually appears to have been put at risk based on the investigation into the incident. The fact that those individuals' information happens to be on the same system that was affected may have no relation to the actual incident or what the incident affected. For example, a threat actor could compromise an employee's email account through a phishing email, and then access documents accessible through that account on a shared file server. The vast majority of files and data on that file server would not have been accessible to the employee or to the threat actor. However, as drafted, if the covered institution could not determine which files containing personal information actually were accessed within the compromised folder, the institution would be required to notify everyone whose information is stored on that file server (which for Committee members with registered separate accounts may involve millions of records not just for its variable contract owners, but also for its other policyholders as well as policyholders at other financial institutions whose contracts are administered on the same system), even though the vast majority of the information stored on the system clearly was not subject to unauthorized access. This would result in significant over-notification to individuals, which not only would unnecessarily disturb and frighten individuals who likely weren't affected, but would also significantly increase costs and litigation risk for the covered institution and possibly its service providers and other financial institutions whose contracts reside on the system.

For this reason, the Committee requests that the proposed Rule 30(b)(4)(ii) of Reg. S-P be revised to remove the requirement to notify all individuals whose information is on an affected system. Instead, the proposed rule should require that the covered institution notify individuals whose information it reasonably believes was, or reasonably could have been, subject to unauthorized access based on the findings of its investigation.

ii. Allow necessary time to conduct an investigation before notice must be sent to affected individuals.

Additionally, proposed Rule 30(b)(4)(iii) would require covered institutions to notify affected individuals within 30 days of becoming aware of actual or reasonably likely unauthorized access to or use of sensitive customer information. The Committee agrees that prompt notice to affected individuals is imperative. However, the proposed requirement is overly rigid, does not account for the wide variety and complexity of cybersecurity incidents, and would be impossible to meet in many circumstances.

In practice, there are a tremendous number of steps that need to be accomplished between becoming aware of possible unauthorized access to sensitive customer information and being able to issue notifications to those individuals. These steps include needing to respond to and remediate the security incident directly, conduct a forensic investigation to determine what information may have been affected, analyze the affected data to determine what sensitive customer information is contained in affected data, extract or obtain the information needed to make notification to affected users, hire vendors and arrange identity protection services for affected individuals, and actually send the notifications. In some states, it is also a requirement to notify state regulators prior to notifying affected individuals and it is common to receive regulatory feedback on draft notification letters prior to sending them. For many security incidents, it simply will not be possible to accomplish all these steps within 30 days of becoming aware of a possible issue. For example, in the context of a ransomware attack that successfully shuts down systems, remediation requires significant effort and implementation to simply recover systems from back up, including needing to rebuild and redeploy essential systems. Then, once the business has recovered, a full forensic investigation can be made to determine what data may have been subject to unauthorized access or use. In this scenario, it would be practically impossible to comply with the 30-day notice requirement.

While the Commission correctly notes in the S-P Proposing Release that some existing state laws also include a 30-day notice requirement, those requirements generally do not begin to run until a determination has been made that the incident affected residents of that state that will require notice. The proposed 30-day requirement in Reg. S-P, however, would be triggered much sooner in the process (awareness of reasonably likely access to any customer information), and so is not comparable or consistent with existing 30-day timelines under state law.

The Committee requests that proposed Rule 30(b)(4)(iii) of Reg. S-P be revised to require that individual notices be provided no later than 30-days from a determination that actual or reasonably likely unauthorized access to sensitive customer information has occurred. A revised Rule 30(b)(4)(iii) could also separately require covered institutions to conduct a prompt investigation of potential incidents of unauthorized access or use of customer information, which would address the Commission's expressed concern about lengthy investigations unduly delaying customer notification. Taking this approach would better align with existing standards (such as the NAIC Insurance Data Security Model Law and many state breach notification statutes), would account for the significant practical challenges faced by covered institutions seeking to respond to cybersecurity incidents, and still would provide strong requirements that require timely notification of affected individuals.

iii. Covered institutions should be able to delay notification at the request of law enforcement.

The Committee also notes that the permitted delay of notification at the request of law enforcement under proposed Rule 30(b)(4)(iii) is too narrowly tailored. As drafted, covered institutions would only be permitted to delay for up to 30 additional days if specifically requested by the Attorney General of the United States on the basis of substantial risk to national security. Requests by local or state police, or even other federal agencies, would not be sufficient. Likewise, delays in the interest of pending law enforcement action or to address concerns that do not rise to the level of "national security" would also not be sufficient. This requirement, which would not prevent law enforcement from directing covered institutions to delay notification beyond what is provided for in the S-P Proposing Release, would simply put covered institutions in the difficult and unnecessary position of being subject to directly conflicting regulatory prerogatives. It could also have negative effects on law enforcement matters if notice is not able to be delay as needed. Accordingly, the Committee requests that proposed Rule 30(b)(4)(iii) be revised to simply allow for notice to be delayed upon the written request of a federal or state law enforcement agency.

iv. Notices should not be required to include a specific office to contact for more information.

Proposed Rule 30(b)(4)(iv) would require that notices sent to affected individuals include the name of a specific office to contact for further information and assistance. This requirement would appear to require covered institutions to task a single internal office and its staff with fielding inquiries from affected individuals, which could be voluminous and likely outside of the normal functions and expertise of any single office within the covered institution. It is unclear what purpose or benefit this requirement would have for affected individuals, while simultaneously placing significant burdens on the internal operations of the covered institution. Rather, it should be sufficient to provide a general inquiry line where affected individuals can ask questions and receive assistance. Such an approach would be consistent with current business practice, where companies hire vendors who offer specialized breach response call centers to handle consumer inquiries. The staff of these call centers are equipped with sufficient information to answer questions about the incident, and are specifically trained and familiar with offering assistance to affected individuals, including working to remediate possible instances of actual identity theft. The requirement to include contact information for a specific office to contact should be deleted.

v. *Consider whether an SEC specific notice obligation is warranted at all.*

The Committee notes that there are existing data breach notification laws in place in all 50 states. Those laws already require covered institutions to provide notice to individuals whose personal information has been subject to a data breach as defined by that state's law. These laws are specifically designed to ensure individuals receive clear and consistent notice when they are at risk of identity theft or fraud as a result of a breach. The new notice requirement proposed under Proposed Rule 30(b) would simply add another layer on top of these existing requirements and would likely go entirely unnoticed by consumers, while complicating compliance efforts for covered institutions and raising additional compliance and legal risk. Although some state laws do provide exemptions from their state specific notice requirements where a notice is provided consistent with requirements under the Gramm-Leach Bliley Act (GLBA), most do not. This proposed new requirement would not serve to preempt those

generally applicable state notice requirements, and would not establish a new singular standard. It would just be another variation on existing requirements to be accounted for, with limited real benefit to affected individuals.

The Committee submits that this new notice requirement may not be warranted at all. But to the extent that it stands, the Committee urges the Commission to deem compliance with substantially similar notice requirements at the state and/or federal level to satisfy the notice requirements in proposed Rule 30(b)(4)(ii) of Reg. S-P. The goal of the notice requirement should be to inform customers of the unauthorized access of their personal data so that they may take appropriate actions, not to inundate consumers with overlapping and confusing notices about the same incident, which may or may not have affected them directly.

3. Refine and clarify key definitions.

*i. Clarify the Definition of "**Sensitive Customer Information**" by specifying what types of information specifically are included in the definition and avoid the use of the undefined term "compromise".*

Proposed Rule 30(e)(9) would define "Sensitive Customer Information" to include **"**any component of customer information alone or in conjunction with any other information, the *compromise* of which *could create a reasonably likely risk of* substantial harm or inconvenience to an individual identified with the information." (Emphasis added.) This formulation is unclear, and provides little guidance to covered institutions regarding what information the Commission will view as being included in the definition. While the examples provided in proposed Rule 30(e)(9)(ii) are appreciated, a short and non-exhaustive set of examples for such a broadly worded standard provides little guidance on the outside bounds of what does or does not constitute Sensitive Customer Information. What makes this standard particularly broad and unclear as drafted is that it includes not only information which actually creates "a reasonably likely risk" of substantial harm or inconvenience, but also information which "*could* create" such a risk. It is unclear how this double-risk standard would function in practice, or what concerns this formulation is intended to address. This definition is also uncommonly broad in that it provides that a single piece of information in isolation could also be enough to trigger a notification obligation. Because of the uncertain meaning and the apparent broad scope of this standard, covered institutions would likely err on the side of over-notifying individuals of incidents, which would be counter to the Commission's intent to avoid over-notification of consumers as noted in the S-P Proposing Release.[3]

The Committee requests that proposed Rule 30(e)(9) be revised to specify the types of identifying information that constitute Sensitive Customer Information as raised in question 37 of the S-P Proposing Release.[4] In particular, the Commission should define "Sensitive Customer Information" to consist of an individual's name or first initial and last name in conjunction with a specific list of types of personal information that are widely recognized as creating a risk of identity theft, such as social security number and state ID numbers.. Such an approach would harmonize Reg. S-P with the approach taken in existing federal and state breach notification laws, and would provide needed clarity around what the Commission views as Sensitive Customer Information. This would also allow covered institutions to align their

---

[3] See S-P Proposing Release at 47 ("We do not believe that notification would be appropriate if unauthorized access to customer information is not reasonably likely to cause harm. . . . Moreover, the large volume of notices that individuals might receive in the event of unauthorized access to such customer information could erode their efficacy.")

[4] See Id. at 50.

practices with the Commission's expectations. One possible approach is to adopt the definition of "Sensitive Customer Information" from the Interagency Guidelines[5], which defines it as:

> "a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to logo onto or access the customer's account, such as user name or password or password and account number."

We also note that the definition uses the term "compromise," which is undefined and not used elsewhere in the proposed amendments. The intended scope of this term is unclear. The term "compromise" should be replaced with "unauthorized access or use," consistent with the language used elsewhere in proposed Rule 30. Moreover, other state and federal authorities do not use the term "compromise" when discussing unauthorized access or use of personal information.

*ii. Revise the definition of "**Substantial Harm or Inconvenience**" to clarify that harm or inconvenience must be "substantial," not merely "more than trivial."*

Proposed Rule 30(e)(11) would define "Substantial Harm or Inconvenience" as: "personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial, including theft, fraud, harassment, physical harm" and other types of harm.[6] (Emphasis added.) Responding to Question 44 in the S-P Proposing Release,[7] the Committee does not believe that "more than trivial" is the correct standard. While we recognize that the term "Substantial Harm or Inconvenience" is taken directly from the GLBA as noted in the S-P Proposing Release,[8] the proposed standard would set a very low bar that would require second-guessing by financial institutions and their service providers and could cause covered institutions to include even minor inconveniences within the definition of "Substantial Harm or Inconvenience" simply because they are "more than trivial."

Accordingly, this standard, particularly when taken in conjunction with the double-risk standard in the definition of "Sensitive Customer Information" discussed above, would seem to sweep a huge array of potentially minor effects on customers into the notice requirements of proposed Rule 30. Indeed, it is hard to imagine any instance of unauthorized access or use of customer information that could not create a reasonably likely risk of more than trivial inconvenience, and therefore would not require notification. Accordingly, not only would the proposed standard result in notification of functionally all instances of unauthorized access or use, it would be contrary to the "substantial harm or inconvenience" standard articulated in GLBA. The proposed standard would functionally replace "substantial" with "any." We also note that, as drafted, it is unclear whether the "more than trivial" standard applies at all to instances of personal injury or financial loss.

---

[5] Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); and 12 C.F.R. Part 364, app. B (FDIC).

[6] S-P Proposing Release at 52 (emphasis added).

[7] Id. at 54.

[8] Id. at 8.

The Committee requests that proposed Rule 30(e)(11) be revised to align with the "substantial harm" standard articulated in GLBA by redefining "Substantial Harm or Inconvenience" in proposed Rule 30(e)(11) to mean "substantial personal injury, financial loss, or expenditure of effort or loss of time . . . ." and deleting the phrase "more than trivial."

*iii. Clarify the scope of information subject to the requirements of proposed Rule 30, and the obligations of financial institutions when acting as a **service provider**.*

As drafted, there appear to be overlapping and potentially conflicting statements defining the scope of information subject to the requirements of Rule 30. Rule 30(a) of the S-P Proposing Release notes that Rule 30 would be intended to apply to all customer and consumer information that a covered institution maintains or possesses, regardless of whether such information is about the covered institution's own customers or is information it handles on behalf of another financial institution. Separately, and in conflict with proposed Rule 30(a), proposed Rule 30(e)(5) of the S-P Proposing Release would define "customer information" to mean any Nonpublic Personal Information about a customer of any financial institution (not just the covered institution itself) that is handled or maintained by the covered institution or on its behalf. The plain language reading of these two subsections directly conflict with each other. Rule 30(a) appears to limit the scope to information actually possessed by the covered institution, regardless of whether the covered institution processes that information for its self (i.e. controls the data and has a direct relationship with the customer whose data it processes) or for another (i.e. acts solely as a service provider or processor of the data and does not have a direct relationship with the customer associated with the data). In both instances, as long as the covered institution possesses the data, it would be subject to all of the requirements under Rule 30, including notification requirements. In contrast, newly proposed Rule 30(e)(5) extends the definition of customer information not just to information in the covered institution's possession (i.e. that it directly handles or maintains), but to any customer information handled or maintained on its behalf (i.e. information that it does not directly possess, but which another entity processes on its behalf).

These statements create uncertainty as to the fundamental scope of customer information covered by proposed Rule 30 because it is unclear whether a covered institution would be responsible only for customer information that it possesses regardless of on whose behalf it possesses that information, or only for information processed on the covered institution's behalf regardless of whether it actually possesses that information. This dynamic could also create duplicative notification obligations where there is unauthorized access to sensitive customer information that is held or maintained by one financial institution on behalf of another, since proposed Rule 30 notification obligations would appear to apply to both financial institutions simultaneously even though only one set of customer information was accessed.

The Committee requests that the Commission clarify the scope of customer data subject to the requirements of proposed Rule 30 to be the customer information of the covered institution's own customers whether processed by the covered institution directly or on its behalf. This approach would align the responsibility to protect customer information with the entity with whom the customer has chosen to transact, and ensure that customer information is required to be protected appropriately without creating overlapping or duplicative obligations. Separately, to the extent a covered institution processes customer information on behalf of another financial institution, it should have a separate obligation to promptly notify the other financial institution of unauthorized access or use of its customer information in lieu of an obligation to directly notify affected individuals. This approach would harmonize Reg. S-P with the approach taken by the leading existing privacy and cybersecurity laws, such as the controller to

processor framework under the European General Data Protection Regulation and the business to service provider framework under the California Consumer Privacy Act.

*iv. Revise the definition of "**Service Provider"** to exclude affiliates of the covered institution.*

Proposed Rule 30(e)(10) would define "Service Provider" as: "any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution."[9] As currently defined, this term would include affiliates within the same holding company that provide IT and cybersecurity services on a group-wide basis. Cybersecurity and privacy programs, including service provider management, are frequently structured and operate on a group-wide basis. Specifically with respect to Committee members' variable contract business, where a separate account and one or more of its service providers (such as the insurance company and the principal underwriter for the separate account) are part of the same group, the Committee believes that such entities should not be considered the separate account's service provider for purposes of proposed Rule 30. The Committee notes that it serves no practical or policy purpose to require a separate account to treat affiliated or controlling entities as service providers in circumstances where the entities participate in the same cybersecurity program as the separate account, where the program is likely run by the same people and employs the same cybersecurity measures throughout the enterprise. The Committee requests that proposed Rule 30(e)(10) be revised to specifically exclude affiliates and other entities under common control with the covered institution.

4. Avoid prescribing specific contractual terms for service provider contracts.

Proposed Rule 30(b)(5) would require a covered institution to include specific terms in any agreement with a service provider, including providing notice of a breach of security resulting in unauthorized access to a "customer information system" in order to "enable the covered institution to implement its response program." Accordingly, it appears that this provision would prohibit a covered institution from using service providers that are unwilling to agree to the prescribed terms. In practice, this will often force covered institutions to choose between either using the best and most dependable service providers or complying with these regulatory requirements, since many leading service providers (such as cloud service providers) do not negotiate the standard terms of their services with customers and those standard terms generally would not meet the proposed contractual requirements. The Committee recognizes and supports the importance of covered institutions having appropriate policies and procedures to manage the cybersecurity and privacy risks posed by service providers the process their customer information. However, the Commission should not define specific contractual requirements within its regulations, which would create on overly rigid approach and hinder the ability of covered institutions to use the best vendor available.

5. Clarify who within the covered institution the Commission will deem to be responsible for oversight of the incident response program in proposed Rule 30(b)(3) – (5).

Ever since Rule 38a-1 under the IC Act was adopted in 2004, compliance with the requirements of Reg. S-P has been the responsibility of the registered separate account's Chief Compliance Officer (CCO), as required by Rule 38a-1. If this requirement continues to stand, the CCO would also be

[9] S-P Proposing Release at 244.

responsible for oversight of the new provisions of Reg. S-P regarding the incident response program, service provider contractual terms, and notice requirements set forth in the S-P Proposing Release.

However, the IM Cybersecurity Release[10] would also impose incident response and notice requirements on registered separate accounts under recently proposed Rule 38a-2. Those obligations would likely not be subject to oversight by the Rule 38a-1 CCO, but rather would be overseen by other appropriate personnel at the insurance company.[11]

This issue of overlapping oversight responsibilities is a serious issue for Committee members. Of particular concern is the question of how the Commission will view the division of oversight responsibilities during separate account exams. Will the Commission permit registered separate accounts to determine the person or persons most appropriate for the oversight responsibility or will it expect the Rule 38a-1 CCO to oversee both Rule 38a-2 and all of Reg. S-P, including the incident response policies and procedures? The issue takes on more urgency given the overlapping requirements for incident response policies and procedures in proposed Rule 38a-2 and proposed Rule 30(b)(3) in Reg. S-P.

The Committee asks the Commission to provide thoughtful guidance on its expectations for oversight in order to ensure the orderly implementation of and compliance with the overlapping requirements set forth in the Reg. S-P Proposing Release and in the IM Cybersecurity Release.

* * *

The Committee appreciates the time and resources the Commission and its staff have devoted to this rule proposal, as well as the opportunity to provide the Committee's views to the Commission. We also appreciate the Commission's careful consideration of the comments expressed herein. If you have any questions about our comments please contact Stephen Roth (202-383-0158), Mary Jane Wilson-Bilik (202-383-0660), or Alexander Sand (512-721-2721).

Respectfully submitted,

Eversheds Sutherland (US) LLP

Eversheds Sutherland (US) LLP

FOR THE COMMITTEE OF ANNUITY INSURERS

cc: William A. Birdthistle, Director, Division of Investment Management
Haoxiang Zhu, Director, Division of Trading and Markets
Sarah G. ten Siethoff, Deputy Director, Division of Investment Management
Thoreau Bartmann, Co-Chief Counsel, Division of Investment Management
Emily Westerberg Russell, Chief Counsel, Division of Trading and Markets

[10] See discussion at p. 35-38 in IM Cybersecurity Release.

[11] The Committee has asked the Commission to clarify oversight responsibility for proposed Rule 38a-2 in its comment letter to the Commission dated April 11, 2022.