EVERSHEDS SUTHERLAND

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

April 11, 2022

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

Re: **Proposed Rule: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies**
File Number S7-04-22

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. 33-11028; 34-94197; IA-5956; IC-34497 (February 9, 2022) (the "Proposing Release") for comments on new cybersecurity risk management rule 38a-2 under the Investment Company Act of 1940 (the "Investment Company Act"), as well as amendments to Forms N-4 and N-6.

Committee members applaud the Commission's goals in proposing the cybersecurity risk management rules and form amendments. In the Proposing Release the Commission asks for comments on many aspects of the proposed rules 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' consideration of some of the Commission's requests for comment, so that the proposed rules can be effectively and efficiently implemented by individual Committee members in the context of the variable annuity contracts that they offer.

In discussing the application of the new rules in the Proposing Release, the Commission appears to have focused its attention primarily on the operational impacts of proposed rule 38a-2 and form amendments on registered mutual funds (open-end management investment companies) and registered investment advisers, leaving unclear the application of some of the provisions of the rules in the variable annuity separate account context.

Most variable annuity separate accounts are organized as "unit investment trusts" ("UITs") that do not have officers, directors or employees. Variable annuity UIT separate accounts operate within the requirements of the Investment Company Act as the top tier in a

[1] The Committee is a coalition of many of the largest and most prominent issuers of annuity contracts. The Committee's current 30 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 three 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/.

The Committee's comments advanced in this letter relate specifically to variable annuity contracts, although the comments should be equally relevant to variable life insurance policies.

two-tier structure, with the bottom tier typically comprised of dozens of underlying registered mutual funds. This letter identifies for the Commission additional considerations the Committee believes should be taken into account in determining how proposed rule 38a-2 should apply to insurance company variable annuity UIT separate accounts.

1. Request that the Commission clarify that UIT separate accounts and underlying funds are not service providers to each other

The Committee requests that the Commission clarify that UIT separate accounts and their underlying funds are not service providers to each other within the meaning of rule 38a-2 and the proposed amendments to Forms N-4 and N-6 in order to avoid unnecessary duplication and to reflect the reality of the relationship between UIT separate accounts and their underlying funds.

This request is based on the fact that both UIT separate accounts and underlying funds are registered investment companies under the Investment Company Act that are bound together in one product offering. Each of the UIT separate accounts and the underlying funds would be independently subject to the requirements of rule 38a-2 and to new form disclosure requirements of significant fund cybersecurity incidents. If each UIT separate account is required to treat the dozens of underlying funds as service providers, the UIT separate account would be required to take on significant compliance obligations with respect to each of those funds' compliance with rule 38a-2 that is disproportionate to the cybersecurity risk posed by underlying funds to UIT separate accounts and would duplicate the funds' own obligations under rule 38a-2.

Each UIT separate account would also be mandated to add provisions to its participation agreements with each underlying fund requiring the separate account to oversee the funds' compliance with rule 38a-2, a role reserved in the rule for the underlying fund's board of directors. In addition, it would require the underlying fund to disclose each significant fund cybersecurity incident to the UIT separate account for disclosure in the UIT separate account's Form N-4 prospectus, while the underlying fund also would be required to disclose these same incidents in its own Form N-1A prospectus, leading to potential confusion and unnecessary redundancy with little benefit to investors.

UIT separate accounts and their underlying funds do not operate as typical service providers that "receive, maintain or process" information about the other's business or operations. UIT separate accounts and underlying funds each have their own operations with limited overlap among them that involves the underlying funds providing their daily net asset values (which is public information) to the UIT separate accounts so that the UIT separate accounts can calculate their accumulation and annuity unit values. UIT separate accounts also share limited, non-personal information with the underlying funds regarding the UIT separate account's daily aggregate buy or sell order of underlying fund shares, and may be required by a fund to share limited personal information about contract owners in response to a Rule 22c-2 request from the fund. Whatever systems are involved in these functions would already be subject to the UIT separate account's or the underlying fund's own cybersecurity risk policies and procedures under rule 38a-2, without imposing a duplicate layer of obligations that would be triggered by the "service provider" designation.

For these reasons, the Committee requests that the Commission clarify that UIT separate accounts and underlying funds are not service providers to each other.

2. Request that the term "Service Provider" be clearly defined to allow a risk-based approach and to exclude affiliated and controlling entities

Proposed rule 38a-2 does not define "service provider" *per se*. However, proposed rule 38a-2 would require a UIT separate account to identify and assess the cybersecurity risks, and oversee the compliance with rule 38a-2, of its service providers "that receive, maintain or process [separate account] information, or are otherwise permitted to access [separate account] information systems and any [separate account] information residing therein…." UIT separate accounts would also be required to record and disclose certain cybersecurity incidents involving its service providers.

The Proposing Release requests comment in Item 14 on whether these requirements should apply only to "named service providers," which includes the service providers of the UIT separate accounts identified in rule 38a-1 under the Investment Company Act, namely, the insurance company, the administrator and the principal underwriter for the UIT separate account.

Risk-based approach: The Committee recognizes that there are entities, other than the named service providers, that provide services to UIT separate accounts and "receive, maintain or process" separate account information or are permitted access to the separate account's information systems. Some of these entities, but not all, may pose material cybersecurity risks to the separate accounts and their investors. The likelihood of material cybersecurity risk may arise from the volume and type of information shared, the level and duration of system access, or the criticality of the function performed.

Some cloud providers and reinsurers that process variable contract information could be examples of such material service providers. However, as currently articulated in the Proposing Release, the phase "service providers that receive, maintain or process separate account information" has no sense of proportionality to the magnitude of the risks posed by the service provider, and so has the potential to be significantly over inclusive. The definition of service provider should incorporate a risk-based approach to determining the extent to which third parties should be subject to service provider due diligence and oversight requirements, which would allow UIT separate accounts to focus their resources and attention on those third parties where the magnitude and likelihood of cybersecurity risk warrants treatment as a full service provider under Rule 38a-2, and would thereby further the Commission's goals of taking a risk-based approach to managing cybersecurity risks.

Excluding affiliated and controlling entities: Where a UIT separate account and one or more service providers (such as the insurance company and the principal underwriter for the UIT separate account) are part of the same enterprise cybersecurity program, the Committee believes that such entities should not be included in the UIT separate account's service provider oversight program in rule 38a-2, so long as the entities are covered by an enterprise cybersecurity program that also includes the UIT separate account. The Committee notes that it serves no practical or policy purpose to require a UIT separate account to include affiliated or controlling entities in its service provider oversight program in circumstances where the entities participate in the same cybersecurity program as the UIT separate account, where the program is likely run by the same people and employs the same cybersecurity measures throughout the enterprise, and where the enterprise cybersecurity program is already subject to the requirements of rule 38a-2 by virtue of the program covering the UIT separate account.

3. Request that the specific contract requirements for service providers in proposed rule 38a-2(a)(3)(ii) be encouraged, but not required

Proposed rule 38a-2(a)(3)(ii) would require that UIT separate accounts enter into a contract with each of its service providers specifying that the service provider will implement and maintain appropriate cybersecurity measures that are designed to protect the UIT separate

account's information and systems. The appropriate measures required of service providers must include the practices required of the separate account by rule 38a-2, such as conducting risk assessments, identifying and overseeing service providers and maintaining cybersecurity incident response and recovery measures. Service providers would also be required to report any Significant Fund Cybersecurity Incident to the UIT separate account for disclosure in the UIT separate account's prospectus.

There is a significant risk that major service providers, such as cloud providers or infrastructure companies, will not be willing to enter into contracts that include the specific terms mandated by proposed rule 38a-2(a)(3)(ii). Requiring UIT separate accounts to use only service providers that are willing to enter into such specific terms could limit UIT separate accounts' ability to choose the service providers that best meet their needs, and could result in less resilience and security overall if certain high-quality service providers are simply unwilling to commit to the specified contract terms.

For these reasons, the Committee requests that the Commission revise proposed rule 38a-2 to encourage UIT separate accounts to enter into contracts with its service providers that contain the specific terms specified in the proposed rule, but not to require each service provider to agree to each of the requirements.

4. Request that the definition of "cybersecurity incident" include a materiality threshold

Proposed rule 38a-2(a)(5)(ii) and (e)(5) would require a UIT separate account to document the occurrence of "any cybersecurity incident", including records related to any response and recovery from such incident, and retain them for 5 years. The proposed rule defines "cybersecurity incident" very broadly as an "unauthorized occurrence on or conducted through a fund's information system that jeopardizes the confidentiality, integrity or availability of a fund's information system or any fund information residing therein."[2] This definition could require documentation of even minor incidents and easily thwarted attempts to penetrate the network of a large company, which often amount to hundreds, if not thousands, of minor incidents each day. Such incidents are unfortunately a routine part of doing business today that many companies detect and track to some extent as part of their cybersecurity programs. However, mandating that each such incident be documented to the extent required under the proposed rule would create a significant operational burden with little added utility to managing cybersecurity risk. The Committee recommends that the definition of "cybersecurity incident" be clarified to include a materiality threshold[3] to carve out minor and routine events.

5. Request that the definition of "Significant Fund Cybersecurity Incident"(SFCI) be revised, the disclosure requirements scaled back and guidance provided on the timing of prospectus disclosures

The definition of SFCI should be clarified and the prospectus disclosure requirements should be scaled back. Proposed rule 38a-2(f) defines a SFCI as a "cybersecurity incident that significantly disrupts or degrades the separate account's ability to maintain crucial operations or leads to the unauthorized access or use of separate account information, where the unauthorized access or use of separate account information results in substantial harm to the separate account or an investor whose information has been accessed." (emphasis added.)

First, the Committee urges the Commission to provide guidance on the meaning of the terms "significantly" and "substantial harm" because they are not defined in the rule, and to apply the concept of "materiality" to when the harm to investors must be disclosed. As the

[2] See proposed rule 38a-2(f).

[3] The U.S. Supreme Court's formulation of materiality in Basic, Inc. v. Levinson, 485 U.S. 224 (1988), would provide a practical and useful benchmark in this context.

proposal currently stands, harm to one investor could result in extensive prospectus disclosure, despite having no material effect on the normal operations or overall cybersecurity of a UIT separate account. For UIT separate accounts and other registered investment companies with tens of thousands of investors, this could result in over-disclosure of security incidents that would go beyond what is meaningful or useful to investors, while creating the risk of painting a misleadingly negative picture of the separate account's cybersecurity risks.

Second, as proposed, UIT separate accounts would be required to discuss in its prospectus any ongoing SFCI that is currently affecting the UIT separate account, the insurance company, or any of the UIT separate account's service providers. This requirement is ill-fitted to the nature of cybersecurity investigation and response in practice and will serve predominantly to expose insurance companies and UIT separate accounts to greatly heightened litigation risk. Investigation of a cybersecurity breach necessarily requires assuming the worst in early stages of the investigation and relying on investigation findings to determine the true scope of an incident and its effects. In almost all cases, the understanding of an incident will evolve rapidly and consistently over the course of investigation, with some findings ending very far from where they started, including that what was thought to be a potentially serious incident was actually very limited. Requiring prospectus disclosure of ongoing incidents will require public disclosure, and potentially market moving disclosure, based on incomplete information that may turn out to be very different than what the investigation ultimately finds. Such disclosures would serve little useful purpose to investors, while exposing UIT separate accounts and other investment companies to substantial potential liability. Accordingly, ongoing incidents should be excluded from required prospectus disclosures.

Third, the Proposing Release would require prospectus disclosure of any SFCI that occurred or is occurring at any service provider. Depending on the breadth of the asked-for definition of "service provider," requiring a UIT separate account to disclose harmful incidents at a third party service provider is unprecedented and could be unworkable. The concern is that this disclosure requirement could have the unintended consequence of causing high quality service providers to abandon servicing UIT separate accounts if they must run the risk of reputational damage and the possible collateral consequences of class action lawsuits in some states from such admissions.

Fourth, the detailed prospectus disclosure of SFCIs required in the proposed Form N-4 and Form N-6 amendments on the scale envisioned by the Proposing Release[4] could encourage bad actors by giving them insights into the interconnectedness and interdependency of different entities in the financial markets, potentially providing a roadmap to bad actors seeking to disrupt US financial markets. The Committee strongly urges the Commission to cut back on the detail and scope of prospectus disclosure of SFCIs in light of the very real likelihood that such disclosure could lead to the unintended consequence of further enabling bad actors.

Fifth, the requirement to constantly provide and update detailed prospectus disclosure of all SCFIs that have occurred over the past two fiscal years or that are currently ongoing at the UIT separate account, the insurance company and all service providers is overwhelming. If the definition of "service provider" is broad and the proposed level of detail is unchanged, then this requirement could encompass hundreds of entities and require the collection and updating of thousands of pieces of information that would overpower and confuse the investor and require continual updates to the prospectus by means of Rule 497 supplements. The Committee requests that the Commission cut back on the required detailed disclosure of SFCI's and limit

[4] The Proposing Release at 225 would amend Form N-4 to require prospectus disclosure of all SCFI's that have occurred within the last 2 fiscal years, as well as any ongoing incidents, that must include: (i) all entities affected; (ii) when the incident was discovered and whether it is ongoing; (iii) whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; (iv) the effect of the incident on the UIT Separate Account's operations; and (v) whether the UIT Separate Account, the insurance company or any service provider has remediated, or is currently remediating, the incident.

prospectus updates to the annual update so that prospectus disclosure can be succinct and properly vetted for accuracy and completeness.

For these reasons, the Committee requests that the Commission revise the definition of "Significant Fund Cybersecurity Incident" to include the concept of "materiality" in the number of investors significantly harmed by the SCFI, scale back the requirement that prospectus disclosure of SCFIs must include all ongoing incidents and be applied to all service providers, and reduce the extensive prospectus disclosure of SCFIs by clearly stating that a UIT separate account is not required to disclose details that could increase the cybersecurity risks facing the regulated entity and that it need only amend prospectus disclosure on such incidents on an annual basis.

6. Request that the Commission amend the 48 hour SFCI notification rule to align with existing standards and avoid overly burdensome and unhelpful update requirements

The Committee agrees that prompt notice to the Commission regarding truly material cybersecurity incidents is an important part of protecting investors and allowing the SEC to support registered funds and advisors when responding to cybersecurity attacks. However, the current formulation of proposed rule 204-6 under the Investment Advisers Act undercuts this goal in practice by establishing a reporting framework that is too rigid, too quick, and too subjective and that will result in pulling focus and resources away from the substantive response and remediation of cybersecurity incidents. The requirement to provide an initial report of any SFCI within 48 hours of "having a reasonable basis to conclude that any such incident has occurred or is occurring" should be amended to better align with existing standards and best practices by requiring notice of SFCI's to be made within 72 hours from a *determination* that a reportable SFCI has occurred or is occurring.[5]

The 48-hour deadline is overly short and does not reflect the realities of incident investigation and reporting, which require time to identify and extract the salient facts and implications of an attack pulled from a complex and technical morass of integrated systems and data. An overly short reporting deadline will result in trapping funds and advisers between issuing required but premature and unhelpful initial reports about incidents that may well turn out *not* to be significant and issuing tardy but meaningful initial reports to the Commission about true SFCIs. A 72-hour deadline would instead align with existing incident reporting requirements under similar reporting regimes[6], and reflect a recognized balance between the time needed for fact discovery and to prepare meaningful notices and the time needed for prompt notice to regulators.

This 72-hour reporting obligation should run from a *determination* that a reportable SFCI has occurred or is occurring, as opposed to after "having a reasonable basis to conclude that any such incident has occurred or is occurring."[7] The proposed reasonable basis standard, which would apply to broad organizations engaged in a complex and multi-layered emergency

---

[5] For instance, Section 6.A. of the Insurance Data Security Model Act promulgated by the National Association of Insurance Commissioners and adopted in numerous states requires insurers to notify the Insurance Commissioner in their state of domicile within 72 hours of the determination that a cybersecurity event has occurred.

[6] See, e.g., 23 NYCRR § 500.17(a); EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Art. 33.

[7] We note that Federal banking agencies (the Office of the Comptroller of the Currency at the Department of the Treasury, the Federal Reserve System, and the Federal Deposit Insurance Corporation), in a recent rulemaking requiring notification of computer-security incidents to the agencies, replaced their proposed "good faith belief" notification standard with a "determination" standard. "Use of the term 'determined' allows the bank…. time to examine the nature of the incident and assess the materiality of the disruption." "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," Federal Register, Vol 86, No. 223, 66424 at 66434 (Nov. 23, 2021).

response process involving many individuals and third parties, would be very difficult, if not impossible, to get right in practice. There are simply too many people and too many information inputs involved in incident response for legal and compliance professionals to identify the moment that an organization as a whole may have a reasonable basis to know that a new incident constitutes an SFCI. Additionally, the technical personnel who occupy the front lines of incident response are most likely to be the first people in an organization to discover facts that would create a reasonable basis for concluding that an SFCI is occurring. These individuals are rightfully focused not on regulatory reporting but on remediating the incident. Because of this, the "reasonable basis" standard would open funds and advisers to unhelpful second guessing of when the 48-hour period should have started as opposed to when relevant personnel actually had the information necessary to determine that an incident under investigation constitutes an SFCI and must be reported to the Commission. It would also create perverse incentives for funds and advisers to prioritize channeling all incident response information and decision making through legal and compliance functions over and above actually responding to an ongoing cybersecurity event. Funds and advisers would be incentivized to do this so as to avoid the appearance that there was a reasonable basis to know of an SFCI earlier than when the organization was actually capable of reporting that incident to the Commission in practice.

The obligation to amend previously filed notices of SFCIs under the proposal should also be revised to avoid unhelpful and burdensome update reporting obligations that will serve more to consume incident response resources than to provide helpful information to the Commission. The nature of incident response is that often very little is known about the full scope and impact of an incident at the beginning of the investigation and response process. Material new facts about an incident are routinely discovered on a daily or even hourly basis. Accordingly, the 48-hour update obligation would in practice create a requirement to provide the Commission with daily blow-by-blow reports of SFCI investigation and remediation progress that would be burdensome on advisers and exceed the ability of the Commission to meaningfully digest and use the information. Instead, the Commission's staff should be given the flexibility to communicate with advisers that report SFCIs to request further updates at a cadence and in a manner they deem appropriate to the particular circumstances, and so that affected advisers are not spending resources on issuing updates that may go unread and unused by the Commission, while not addressing the cybersecurity attack that is harming investors. This disclosure requirement could be accomplished through a broad obligation that advisers must provide updates on previously reported SFCIs as reasonably requested by Commission staff.

The requirement to notify the Commission within 48-hours of a SFCI being resolved or an internal investigation pertaining to such an incident being closed should also be revised to reflect the reality of incident response. In practice, cybersecurity incidents and investigations often do not have a clean and clearly identifiable end point. For example, short term remediation measures meant to respond immediately to an incident will lead to planning for longer-term remediation measures that will be folded into more normal security upgrade, system development, and risk management processes. Similarly, even when a fund or adviser thinks that it has fully remediated an incident, it may keep monitoring systems and dark web activity for a considerable length of time for additional risks or developments that may indicate it missed something. Instead of creating an obligation for advisers to artificially determine when an incident is resolved or closed, the Committee requests that the proposal be amended to require advisers to provide a timely updated Form ADV-C that it believes reflects all final material facts regarding an SFCI, while still leaving an opening for advisers to report further developments as needed.

7. Request that UIT separate accounts not be required to maintain a prescribed "inventory of the components of the fund information systems and fund information residing therein"

The Committee agrees that comprehensive assessment of cybersecurity risks is an important component of cybersecurity risk management policies and procedures, and that such

risk assessment must be based on a strong understanding of a fund's information systems and data. However, proposed rule 38a-2(a)(1)(A) goes beyond this foundational principle of risk management to define a particular approach to carrying out this risk assessment. It would require UIT separate accounts to categorize and prioritize cybersecurity risks through an "*inventory of the components of the fund information systems and fund information residing therein*." This language would appear to require funds to maintain a very detailed list of every system "component" of the fund information systems, which is broadly defined, as well as the specific fund information (also broadly defined) that is held in each component. As drafted, it is also not entirely clear what constitutes a "component" of a system. In practice, it can be quite difficult, if not impossible, to generate current and accurate inventories of every small piece that makes up a fund's information systems and exactly what fund information is stored or processed on each piece. Moreover, such detail is often not necessary or even useful for a fund to understand the systems and types of data it uses, which systems and data are most sensitive or critical to its ongoing operations, and how to protect them. Instead of prescribing the use of a particular inventory, the Committee urges the Commission to amend proposed rule 38a-2(a)(1)(A) to take a more flexible approach that obligates a UIT Separate Account and other funds to categorize and prioritize cybersecurity risks based on the nature of its business, its systems, and the data it collects, generates, and processes.

8. Request that the Commission clarify the relationship between rule 38a-1 and rule 38a-2 in the context of UIT separate accounts

Because rule 38a-2 will be part of the federal securities laws, the presumption is that the Chief Compliance Officer ("CCO") for the separate account's rule 38a-1 compliance program will be required to review and report on the separate account's compliance with rule 38a-2 in the CCO's annual rule 38a-1 report to the depositor (i.e., the insurance company).

However, proposed rule 38a-2(d)(ii) would also require the UIT separate account depositor to oversee the rule 38a-2 cybersecurity risk management report and to receive a report on compliance with rule 38a-2 from the person(s) responsible for compliance with rule 38a-2. The circularity in the construct of having the insurance company depositor of a UIT separate account overseeing (under rule 38a-1) its own role in overseeing rule 38a-2 is duplicative and confusing and could be difficult to implement.

In light of this potential duplication in oversight responsibility, the Committee requests that the Commission streamline the overlapping roles of the depositor in rules 38a-1 and 38a-2, and possibly consider carving rule 38a-2 out from the requirements of Rule 38a-1's compliance program.

* * *

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.

Respectfully submitted,

Eversheds Sutherland (US) LLP

FOR THE COMMITTEE OF ANNUITY INSURERS

cc: William A. Birdthistle, Director, Division of Investment Management
Sarah G. ten Siethoff, Deputy Director, Division of Investment Management