ACLI
Financial Security for Life

May 9, 2022

Via email to rule-comments@sec.gov

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

Re: **Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure**
File Number S7-09-22

Dear Ms. Countryman,

Thank you for the opportunity to provide comments to the Securities and Exchange Commission ("SEC") on the Proposed Rules for public companies regarding cybersecurity requirements. We previously submitted comments on the recent proposal related to Advisors, and many of the points we raised in that comment letter are relevant to this Proposed Rule as well. We will be brief in this letter and limit comments to a few items relevant to both proposals we deem of most importance, plus several items introduced in the Proposed Rule for public companies.

The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 95 percent of industry assets in the United States.

Summary

ACLI member companies appreciate the significance of potential negative impacts from cybersecurity incidents. We take with great seriousness our responsibility for safeguarding our systems, and the personal information contained in those systems regarding our customers, employees, and other stakeholders. Life insurance companies work with state insurance regulators to ensure proper disclosure of cybersecurity risk management practices. ACLI is most concerned about the following aspects of the Proposed Rule: alignment and consistency with existing cybersecurity frameworks, the definitions proffered, and the notice requirements, specifically as they relate to materiality and harm.

Appropriate Alignment and Consistency with Existing Frameworks

ACLI members believe that overall, any cybersecurity proposals generated by the SEC should be appropriately aligned and consistent with existing cybersecurity frameworks. Harmonization with existing frameworks will be extremely helpful in reducing unnecessary compliance burdens. Our members would recommend that overall, the policies and procedures proposed should be less prescriptive and allow flexibility to account for the multiple existing cybersecurity frameworks and various regulatory requirements to which organizations are already subjected. We note that some entities are trying to develop holistic programs that meet all their various regulatory requirements, as well as are appropriate for the size and the risks of the entity, and this is made much easier by harmonization and flexibility. Our members would also urge the SEC not to prescribe one cybersecurity framework over another, as that would be unduly burdensome to entities subject to differing requirements.

Specific items that would benefit from alignment include: (1) notice timeframes; (2) the definition of what constitutes an incident, and when it arises to the level of a reporting requirement; (3) specified coordination among regulators, as where a company has notified its primary regulator; and (4) exceptions for law enforcement investigations.

Materiality Threshold

The definition of "materiality threshold" seems to be inconsistent with other references to "materiality" within the proposal. Of broader concern, the bar for materiality as it relates to cybersecurity incidents appears to be lower than for other reporting requirements. The examples provided involve very broad scenarios that in our view may or may not be material depending on factors such as the preparedness of the company. Without additional context, the examples serve to, intentionally or not, lower the bar for ascertaining materiality. Cybersecurity incidents are of course important matters, but the same can be said of other items subject to reporting—we would urge the SEC to carefully align materiality and notice requirements with existing definitions and guidance.

Notification Requirements

One of our members' primary concerns is with the proposed guidelines regarding notification to the Commission. The proposed four-day requirement we believe to be overly strict and is inconsistent with other federal and state notification requirements. There also is no extension for law enforcement delay/investigation, which we think is necessary. Moreover, it creates a potential scenario where investors are informed prior to the affected data subjects. Notification of business partners could also occur after notification to the SEC, which is undesirable.

We would request a longer notification deadline. Perhaps more important than the duration of the timing itself, is the need to build in some flexibility as to when the clock begins to run. Allowing companies the time to take the appropriate steps to protect consumers and other stakeholders is a critical component of the proposed guidelines. Our members are concerned that a focus on fast reporting takes time away from remediation efforts, and further risk may occur if companies are forced to report before remediation is fully completed. As a final point, it is difficult to envision "standardized and comparable disclosures" resulting from this brief deadline.

Periodic Reporting of Risk Management Practices

The Proposed Rule would require significant amounts of information to be disclosed regarding an entity's programs. We question whether the potential risk generated by this disclosure, and the level of detail envisioned, will outweigh any potential insights for investors.

Aggregate Reporting

The periodic and aggregate disclosures strike us as problematic. Points/questions we would ask to be considered:

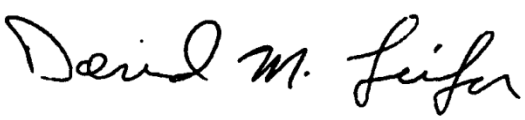
- No other data breach reporting requirement exists like this that we are aware of.
- How operationally would this be administered by an entity?
    - Is there a defined period for aggregate consideration?
    - Is there a defined scope of incidents that should be considered for aggregate?
- Does this aggregated concept provide a roadmap for bad actors of an entity's potential vulnerabilities?
- Specific Feedback Concerning Section F. Periodic Disclosure by Foreign Private Issuers, questions 38 and 39:
    - 38. Should we amend Form 20-F, as proposed to require disclosure regarding cybersecurity risk management and strategy, governance, and incidents? Additionally, should we amend Form 6-K, as proposed, to add "cybersecurity incidents" as a reporting topic? Are there unique considerations with respect to FPIs in these contexts?
    - 39. We are not proposing any changes to Form 40-F. Should we instead require an MJDS issuer filing an annual report on Form 40-F to comply with the Commission's specific proposed cybersecurity-related disclosure requirements in the same manner as Form 10-K or Form 20- F filers?

MJDS filers are already subject to significant regulatory obligations from their securities regulator and industry-specific regulator. We urge the SEC to continue to permit eligible Canadian foreign private issuers to use domestic disclosure standards and documents to satisfy the Commission's requirements and not enact prescriptive cybersecurity disclosure requirements onto Form 40-F filers. Not doing so, would create a significant reporting burden that will slow companies' response to cybersecurity incidents and increase regulatory burden on filers, without necessarily improving upon existing domestic regulatory requirements to develop sound cybersecurity risk management practices.

Conclusion

ACLI Member companies continue to digest the impact of this Proposed Rule, as well as the cybersecurity rules proposed for advisors. Our members welcome the opportunity to continue with a discussion to make sure that the operations of our members are fully considered.

Very truly yours,



Patrick C. Reeder
Deputy General Counsel

David Leifer
Senior Associate General Counsel