June 5, 2023

By Electronic Submission

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

Re: File Number S7–05–23
Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

The American Council of Life Insurers ("ACLI")[1] appreciates the opportunity to respond to the proposed amendments to Regulation S-P[2] ("Proposal") issued by the Securities and Exchange Commission ("SEC") on March 15, 2023. The ACLI recognizes the threat cyber incidents pose to consumers and the United States financial market. The ACLI supports national, uniform, and risk-based cybersecurity standards to combat this threat.

Executive Summary

The ACLI writes this letter in support of the comments jointly issued by the Securities Industry and Financial Markets Association, Bank Policy Institute, Institute of International Bankers, and the American Bankers Association, collectively, the "associations," on the Proposal. The ACLI's members already comply with much of the Proposal's content through state regulations, such as those that require companies to maintain written cybersecurity policies and procedures, respond to cyber incidents, notify authorities and consumers of certain cyber incidents, and dispose of consumer data. However, we are concerned with the Proposal's shortened notification timeframes and expanded scope. As such, we wish to highlight the associations' recommendations to the SEC to consider amendments to the Proposal that would:

1. harmonize and deconflict the Proposal with other proposals and requirements;
2. permit flexibility in third-party service provider contracts;
3. not require that a covered institution provide notice to customers of other financial institutions; and

[1] 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 94 percent of industry assets in the United States.

[2] https://www.federalregister.gov/documents/2023/04/06/2023-05774/regulation-s-p-privacy-of-consumer-financial-information-and-safeguarding-customer-information

4. change the 30-day notification requirement to notification within a reasonable timeframe.

Harmonize and Deconflict the Proposal with Other Proposals and Requirements

The SEC's recently released cybersecurity proposals overlap in some of their requirements. We urge the SEC to both align its cybersecurity proposals with each other, as well as coordinate with existing federal and state regulatory frameworks, to eliminate unnecessary, duplicative, and expensive requirements that would confuse consumers and divert regulated entities from a strong, proactive cybersecurity posture.

The Financial Stability Board's "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting" states:

> Meaningful differences in how different authorities determine their reporting criteria for cyber incidents, use incident information and set their timeframes for reporting an incident pose operational challenges for financial institutions; particularly for financial institutions that operate across many jurisdictions and sectors and are subject to multiple reporting requirements for one incident, with each report tending to trigger follow-up enquiries from each financial authority.[3]

Navigating the maze of cybersecurity regulations at the state, federal, and even international level has become increasingly complex for our members. Targeted, coordinated SEC cybersecurity requirements will help regulated entities to focus their resources on preventing and mitigating cyber incidents. While our members support updating Regulation S-P, we believe that any update should not make compliance with the Regulation exponentially more difficult. The SEC should slow its rule-making process to allow sufficient time to engage with other government agencies and stakeholders. Coordination will help the SEC to construct a framework that will effectively address cybersecurity threats well into the future.

Permit Flexibility in Third-Party Service Provider Contracts

We echo the associations' recommendation that the SEC incorporate a more flexible approach to service provider contracts and notification. While it is standard practice in the insurance industry to include information security provisions in contracts with third-party service providers, a directive to a third-party service provider to notify a covered institution in the event of unauthorized access to a customer information system within 48 hours is not standard. In the early days of containment and remediation it is often difficult to determine exactly what data has been compromised, making the 48-hour timeframe overly short and burdensome. It's also unclear how a third-party service provider's notice would affect a covered entity's reporting requirements. For example, would a third-party service provider's notice to a covered entity automatically trigger the covered entity's 72-hour timeframe to notify regulators?

Furthermore, as a practical matter, it could be difficult to include a 48-hour notification timeframe in a third-party service provider contract, especially with larger companies, such as cloud service providers. Many companies would have to amend their contracts with their third-party service providers, an often costly and time-consuming process. If service providers are unable or unwilling

[3] https://www.fsb.org/wp-content/uploads/P130423-1.pdf (p. 4)

to change their practices, this requirement could cause regulated entities to end essential service provider arrangements with inadequate alternatives.

A more flexible approach would require service providers to notify a covered institution without unreasonable delay after an investigation has been performed by the service provider. Such an approach would harmonize service provider and covered entity requirements.

Not Require that a Covered Institution Provide Notice to Customers of Other Financial Institutions

As insurers and reinsurers, some of the ACLI's members receive seriatim data from other companies. Under the Proposal, it seems that in receiving this data, our members could be obligated to provide notification to the individuals that make up that data, despite having no contract with those individuals nor the individuals' contact information. As the associations' comments state, it would be impractical for a covered institution to identify and contact customers of another institution and could cause customer confusion.

We agree with the associations that an entity experiencing an incident involving sensitive customer information should provide notice to the financial institution that provided the information. Then, the financial institution that has a relationship with a customer should have the responsibility and authority to make its own decision on whether the notification should come from the financial institution holding the customer relationship, or request that the covered institution which experienced the relevant incident provide the requisite notice.

Change the 30-Day Notification Requirement to Notification Within a Reasonable Timeframe

The Proposal would require covered entities to notify impacted individuals as soon as practicable, but no later than 30 days after becoming aware the unauthorized access has occurred. While companies who have experienced a cyber incident work quickly to assess the incident, 30 days after becoming aware is insufficient time to provide a meaningful notification to impacted individuals, particularly in complex cases. The SEC proposes that if a company is unsure about who within the system was impacted, the company should notify everyone who had their information stored on that system. This recommendation effectively means everyone on the system would receive a notice each time there is a reasonable belief of unauthorized access or use. The resulting unnecessary or incomplete notifications would serve only to confuse consumers and desensitize them to notifications.

We support the associations' recommendation that if the SEC decides to keep the 30-day timeframe, the 30-day timer should begin upon the completion of a reasonable investigation and conclusion of the incident response process, rather than from when the covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.

Conclusion

We share the SEC's concerns about cybersecurity in the financial sector. Life insurance companies have robust cybersecurity programs in recognition of their affirmative obligation to protect the security of their customers' personal information and the information systems on which such information is stored. A flexible, coordinated approach to cybersecurity notification requirements will help to ensure that covered entities can focus their resources on preventing and mitigating

cyber incidents. We thank the SEC for considering our comments and join the associations in respectfully requesting that the SEC reconsider the Proposal in accordance with the associations' comments as well as the considerations described above.

Sincerely,

Chanda Brady
Associate Director and Cybersecurity Working Group Lead, ACLI
202-624-2314
chandabrady@acli.com