Mindset

May 9, 2022

By electronic submission to: rule-comments@sec.gov.

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

File No.: S7-09-22

To Whom It May Concern:

I write on behalf of the Insurance Coalition, a group of life and property and casualty insurance companies that share a common interest in federal regulations. In this case, we write in response to the Securities and Exchange Commission's *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* proposed rule for publicly held companies (File No.: S7-09-22). Some Coalition members are publicly traded companies and will be directly affected by this specific proposed rule, and several others will be subject to the Commission's proposed breach notification requirements for investment advisors and the recently enacted Cyber Incident Reporting law included in the FY 2022 Omnibus Appropriations Bill, as well as the various state-level cybersecurity and breach reporting rules.

It is our view that timely and proper cyber incident reporting will help improve our nation's security and are essential elements of our duties of care and good faith to shareholders and/or investors. In that regard, however, we are conscious of the importance of breach notification to various regulatory agencies at both the state and federal levels, and the potential impact compliance with overlapping regulations can have on our ability to best serve our policyholders.

We welcome this opportunity to comment and look forward to an ongoing dialogue to ensure robust and responsible cyber breach disclosure regulations that appropriately consider the insurance industry's unique regulatory framework.

I. Vertical Regulatory Harmonization

Under certain narrow circumstances, insurance companies are subject to specific federal regulations: publicly traded insurers, and in their capacity as investment advisors, are subject to certain SEC regulations; under the Dodd-Frank Act, Insurance Savings and Loan Holding Companies are subject to supervision by the Federal Reserve.[1] However, per the McCarran-Ferguson Act ("McCarran-Ferguson"), enacted in 1945, the business of insurance is regulated by the states.[2]

[1] 31 USC § 313.
[2] 15 USC § 1011.

McCarran-Ferguson sets up a "reverse preemption" regime in which state laws regulating the business of insurance are not preempted unless Congress explicitly states its intention to do so in federal legislation. State regulation of insurance includes solvency regulation and consumer protection regulation. This includes regulating policies, rates, and the conduct of insurance companies in the market through continuous market conduct examinations.

Cyber incident reporting, therefore, falls squarely within the jurisdiction of state insurance commissions. An important issue will be to ensure harmonized regulation between the federal government and the several states with proposed or preexisting cybersecurity regulations. An important means of minimizing compliance costs that do not translate into improved cybersecurity standards or shareholder/investor transparency would be to create safe harbor provisions in terms of notice content. Requiring disclosure on an 8K, or a 10Q or 10K as appropriate, is necessary to put shareholders and investors on notice. However, an overly prescriptive regulation outlining the specific form or contents of the filing will cause insurers to unnecessarily spend time complying with nuanced specifics of various regulatory filings at the state and federal level with no further benefit to our nation's security, shareholders, or investors.

II. Horizontal Regulatory Harmonization

In addition to compliance with state cyber breach notification requirements, many insurers are, or will be, subject to several other federal cybersecurity regulations: a joint rule among prudential banking regulators pertaining to computer-security incident reporting,[3] the Commission's proposed cyber breach reporting rule for registered investment advisors,[4] and potentially the forthcoming cyber incident reporting rule for critical infrastructure industries to be promulgated by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).[5]

While this proposed rule requires entities to report a material breach within four business days, the banking agency computer-security incident reporting rule requires "notif[ication]...as soon as possible when the bank service provider determines that it has experienced a computer-security incident,"[6] the RIA rule would require notification within 48 hours,[7] and CISA's forthcoming rule, per statute, will require notification within 72 hours.[8]

Again, each regulation serves an important policy goal. And alerting necessary stakeholders in a timely manner is essential. However, compliance with various—and perhaps at times duplicative or conflicting—requirements in each regulation in such a short amount of time can distract from immediate goals of ensuring the firm's network. Instead, the compliance regime should prioritize substance over form, allow for flexibility through safe harbors or reference to

[3] 12 CFR §53, 225, and 304.
[4] 17 CFR §§ 230, 232, 239, 270, 374, 275, and 279.
[5] Division Y, H.R. 2471, 117th Congress (2021-2022): Consolidated Appropriations Act, 2022.
[6] *See supra*, note 3.
[7] *See supra*, note 4.
[8] *See supra,* note 5.

other regulatory filings, and strike the right balance of providing necessary disclosures to all relevant stakeholders without distracting from the immediate goals to protect the entity's network.

III. Scope of Compliance

Another crucial means of maximizing regulatory flexibility without compromising safety and transparency is ensuring uniform definitions of key terms, as well as establishing clear guidelines for compliance.

Definition of Relevant Cybersecurity Terms

In addition to allowing for a prudent level of flexibility via safe harbors or harmonization with parallel state and federal regulatory filings, it is imperative that definitions of key terms are also harmonized. Having a clear and uniform understanding of what constitutes cybersecurity, a cyber incident, and what is a cybersecurity expert, will ensure necessary regulatory clarity.

Coordination with other federal agencies to ensure a uniform set of key term definitions will be critical. An easy solution is to adopt definitions from the National Institute of Standards and Technology.[9] Doing so will not only ensure swift compliance following a cyber incident, but also provide a necessary level of clarity to allow for integration of incident reporting into long-term cyber hygiene strategic planning.

Definition of "Materiality"

The proposed rule requires firms to report material cyber incidents, relying on a case law definition of "materiality" as information that "a reasonable shareholder would consider…important."[10] Furthermore, the rule applies a retrospective definition of material by requiring subsequent reporting of an incident if, over time, an incident or incidents become material in the aggregate.[11]

On the one hand, applying a materiality definition from securities case law—including a post-hoc assessment of the aggregate impact of incident(s)—is logical as it seeks to harmonize the Commission's breach notification requirements with other rules and regulations from the SEC. However, the unique, sensitive, and evolving nature of cybersecurity issues does not lend itself to traditional application of securities case law.

Disclosing cyber breaches to the government is a necessary means of ensuring the resilience of our nation's economy, and transparency of our markets. If not properly tailored, however, such disclosures can unintentionally overshare a firm's vulnerabilities if an overly-conservative

[9] Computer Security Resource Center, Information Technology Laboratory, National Institute of Standards and Technology, available at: https://csrc.nist.gov.
[10] TSC Indus. v. Northway, 426 U.S. at 449.
[11] Proposed Item 106(d) of Regulation S-K.

definition of “material” is adopted by the company—thereby exposing the firm to greater risk of cyberattack to the future detriment of shareholders and investors. Conversely, a narrow view of materiality, even if reasonable, could expose an entity to unnecessary regulatory or litigation risk.

Relying on a reasonableness definition of materiality under securities case law in turn requires firms to not only constantly monitor and assess changes in case law definitions, but also to the evolving consequences of a prior cyber incident. This overemphasizes compliance with a regulation, with no direct tangible added benefit to shareholders, to the detriment of allowing for the necessary resources to improve a firm’s cyber posture.

Cybersecurity risk is an evolving and ever-changing threat. Aligning definitions with other securities laws necessarily creates an untenable dynamic where traditional static processes are applied to a fast-paced policy concern. Doing this puts too great of a burden on covered entities and can lead to both over- and under-reporting. This in turn provides inadequate information to the Commission and shareholders, while also exposing firms to unnecessary risks. Instead, clear-cut, standardized, definitions of materiality are needed for ultimate regulatory clarity. And, as discussed above, these definitions can and should be harmonized with other federal and state regulations, and/or a safe harbor allowance for adopting definitions from parallel regulations to which publicly traded firms are subject.

Scope of Coverage

Another issue of particular concern to insurers is ensuring reporting by a parent corporation covers compliance of individual agents, brokers, or other subsidiary entities. A model for this is New York’s Department of Financial Services cybersecurity requirements for financial services companies. Per 23 CRR-NY 500.19(b): “An employee, agent, representative or designee of a covered entity, who is itself a covered entity, is exempt from the Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the covered entity.”[12]

Given the nature of the business of insurance, publicly traded insurers will be subject to both the registered investment advisor cyber breach notification rule, as well as the rule pertaining to publicly traded companies. In other words, a cyber breach of one insurance agency, if owned by a publicly traded parent, necessarily triggers compliance with both regulations. Funneling all filings through a corporate parent will provide organizations with necessary clarity and compliance ease, without detriment to shareholder and investor transparency.

IV. Cybersecurity Expertise for Board of Directors

Under the proposed rule, public companies would be required to disclose the cybersecurity expertise of members of their Board of Directors. The Commission’s proposed rule for investment advisors contains a similar provision. Under the proposed measures, such details

[12] 23 CRR-NY 500.19(b).

would be made available in proxy or informational statements pertaining to the election of Directors. In addition to unclear definitions of “expertise” and the associated compliance costs discussed above, disclosure of cybersecurity expertise without a mandate for cyber experts to serve on a Board, will necessarily signal potential vulnerabilities to cyber criminals—thereby exposing firms to even greater cyber risk.

Having cyber expertise on a public firm Board of Directors is a reasonable means of ensuring good corporate governance. Pursuing this through public, and not private, policy however necessarily creates a Catch-22. Requiring disclosure of cyber expertise on a Board of Directors without a mandate unnecessarily exposes vulnerabilities of firms without cyber expertise, or with limited expertise. This in turn makes reporting a *de facto* mandate for cyber experts to serve on a board for reasonable firms. Mandating cyber experts to serve on public company boards, however, is a potential overreach of the Commission as it denies firms the ability to compete on cybersecurity as a means of protecting shareholders, customers, and investors and ultimately, innovation in both cybersecurity hygiene and corporate governance.

V. Conclusions

The goal of the Commission's proposed rule is laudable, and a necessary complement to other state and federal cyber breach notification regulations to ensure material cyber incidents are properly reflected in share prices of publicly traded firms. However, these goals could be stymied by an overly rigid compliance regime that does not allow for harmonization with existing and forthcoming state and federal regulations. As such, we urge the Commission to adopt a “substance over form” philosophy to breach disclosures and allow for flexibility and harmonization with other filing requirements.

Furthermore, to ensure clarity and swift compliance with reporting following a cyber breach and allow for incident reporting to be integrated into long-term firm cybersecurity strategy, clear, uniform, definitions of key terms and scope of coverage is imperative.

Thank you for your thoughtful consideration.

Sincerely,

Zach Ostro
Senior Director, Cybersecurity Working Group
The Insurance Coalition