Committee on Corporate Reporting

May 9, 2022

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

Re: File No. S7-09-22

Dear Ms. Countryman,

This letter is submitted by Financial Executives International's (FEI) Committee on Corporate Reporting (CCR) in response to the Securities and Exchange Commission's (SEC or Commission) Proposed Rule, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*.

FEI is a leading international organization comprised of members who hold positions as Chief Financial Officers, Chief Accounting Officers, Controllers, Treasurers, and Tax Executives at companies in every major industry. CCR is FEI's technical committee of approximately 50 Chief Accounting Officers and Corporate Controllers from Fortune 100 and other large public companies, representing more than $13 trillion in market capitalization. CCR reviews and responds to pronouncements, proposed rules and regulations, pending legislation, and other documents issued by domestic and international regulators and organizations such as the U.S. SEC, PCAOB, FASB, and IASB.

This letter represents the views of CCR and not necessarily the views of FEI or its members individually.

Executive Summary

We commend the Commission's efforts to build on the existing regulatory framework and interpretive guidance for cybersecurity disclosure, and to enhance the availability and comparability of information disclosed about cybersecurity risk management, strategy, governance, and incidents. As business operations become increasingly reliant on data and technology, cybersecurity continues to be a high priority for registrants, and we support the Commission's focus on increasing transparency to inform investors about the risks and incidents associated with such trends. In our letter, we include specific feedback and considerations on issues related to reporting on an Item 1.05 Form 8-K, information resources that are used but not owned, and the disclosure of cybersecurity incidents that have become material in the aggregate.

Reporting of Cybersecurity Incidents on an Item 1.05 Form 8-K

We support the Commission's decision to use the date on which a cybersecurity incident is deemed to be material, rather than the date of discovery, to trigger the four-business day filing deadline for an Item 1.05 Form 8-K. Focusing disclosure on incidents that are material to investors will streamline the reporting

process and help investors more easily identify decision-useful cybersecurity impacts. In the following sections, we provide specific suggestions and considerations related to materiality determinations, the definitions of key terms, and additional risks that could arise when cybersecurity incident reporting conflicts with other legal obligations or highlights ongoing vulnerabilities.

Materiality Determination

We believe that many registrants already disclose material cybersecurity incidents in accordance with previous SEC staff guidance issued in 2011 and 2018. The proposed amendments will provide additional structure to the reporting of such incidents, which will likely drive greater consistency in the timing and scope of disclosures. However, we believe that registrants may face certain challenges associated with making materiality determinations in accordance with more specific incident reporting requirements. For example, some situations may present clear facts and circumstances that allow management to make a materiality determination coincident with discovering a cybersecurity incident,[1] while at other times, determining the materiality of a cybersecurity incident may be more difficult and require significantly more effort to assess downstream impacts. In these situations, there is an increased risk that judgments made about materiality, particularly judgments based on indicators that correlate with the passage of time (e.g., a sustained decline in sales or increase in costs associated with business interruption) could be second guessed. To mitigate these concerns, we encourage the Commission to affirm in the final rule that, in regard to both the materiality assessments of cybersecurity incidents and the timeliness of such assessments, well-reasoned[2] judgments made by management will be deemed appropriate[3] to the extent they are supportable.

Definitions of Key Terms

We recommend that the Commission remove the concept of "jeopardizes" from the definition of cybersecurity incident. The use of such a term implies that a vulnerability alone could trigger an Item 1.05 Form 8-K, which we do not believe is the Commission's intent. We recommend revising the definition such that it is clear that an Item 1.05 Form 8-K would be triggered only upon the occurrence of a material event, rather than upon the occurrence of an event that creates a vulnerability that could lead to a material event in the future should the vulnerability be exploited.

We also recommend that the Commission work closely with other government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST), to align the definitions of "cybersecurity incident," "cybersecurity threat," and "information systems" to the extent possible. Such coordination is particularly relevant as CISA begins

[1] See page 28 of the proposing release.
[2] On page 24 of the proposing release, the Commission mentions the need for a "well-reasoned, objective approach" when assessing whether a cybersecurity incident is material.
[3] This approach would align with messaging that has consistently been provided by the SEC staff over many years. For example, in response to increased uncertainty during the onset of the COVID-19 pandemic, SEC Chief Accountant Sagar Teotia issued a public statement noting that the Office of the Chief Accountant "has consistently not objected to well-reasoned judgments." Similar remarks have previously been made by the Division of Corporation Finance, such as when Associate Chief Accountant Todd E. Hardiman stated that "reasonable judgment is the foundation of our financial reporting system."

rulemaking on cybersecurity incident reporting in accordance with the recently enacted Cyber Incident Reporting for Critical Infrastructure Act.[4] Under the SEC's proposed rule, determining cybersecurity reporting obligations would necessitate coordination between multiple departments, and relatively consistent definitions across government agencies would streamline cross-functional communication and understanding and promote more consistent disclosure by registrants. Nevertheless, as the Commission contemplates aligning definitions with other organizations, we believe it will be important for businesses to be able to distinguish "material" incidents under SEC reporting from "substantial" incidents under CISA's pending rulemaking given the differences in objectives between the two agencies. In this regard, we recommend that the Commission prioritize clarity over alignment.

Additional Risks from Reporting Cybersecurity Incidents

We understand that the SEC has provided some flexibility around the level of detail that registrants must include when describing the nature and scope of cybersecurity incidents in an Item 1.05 Form 8-K. We also acknowledge that the importance of timely disclosure of cybersecurity incidents for investors may justify not providing for a reporting delay in some situations. However, we believe that there may be circumstances where a reporting delay is warranted due to conflicting legal obligations under federal, state, or international law, or when disclosure is likely to alert a malicious actor and lead to significant incremental harm to a registrant or its employees, customers, or business partners.

In such situations, we recommend that the Commission provide a mechanism by which registrants may, within four business days of determining that a cybersecurity incident is material, submit confidential notice to the SEC informing the Commission of a delay in filing an Item 1.05 Form 8-K. In a subsequent consultation, the registrant and SEC could meet to discuss the facts and circumstances around the delay and determine when filing the Item 1.05 Form 8-K would be appropriate. The following non-exhaustive list includes several examples where we believe such an exception would be appropriate:

- When law enforcement has been granted a court order that restricts a registrant from making public disclosure regarding an ongoing investigation related to the cybersecurity incident.
- In issues of national security where the Attorney General or other competent authority requests a delay in reporting a cybersecurity incident, or a written request for a delay has been submitted to the Attorney General or other competent authority.
- When a foreign regulatory authority restricts a registrant's ability to comply with the proposed cybersecurity incident reporting requirements.
- When disclosing details of a material cybersecurity incident could put a registrant or its employees, customers, or business partners at additional risk of future cybersecurity incidents by alerting malicious actors to significant vulnerabilities and threat channels that might be further exploited.

[4] On March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act, which will require reporting of covered cyber incidents to CISA within 72 hours after a covered entity reasonably believes that a covered cyber incident has occurred.

While we understand the importance of providing investors with information about material cybersecurity incidents in a timely manner, we believe it is important for the Commission, at a minimum, to consider the potential incremental harm to investors that may result when registrants are required to prematurely disclose details of incidents while vulnerabilities still exist. In this regard, we believe that the proposed requirements to (1) describe the effect of an incident on a registrant's operations, and (2) indicate whether an incident has been remediated, could potentially inform malicious actors as to the success or failure of their attacks before appropriate remedial measures are complete. We urge the Commission to conduct additional outreach to fully understand the potential security implications of requiring disclosure in such cases prior to moving forward with the proposed disclosure requirements and issuing a final rule.

Information Resources that are Used but Not Owned

Some registrants may not currently be able to obtain information needed to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them. In some situations, third-party contracts may need to be aligned with the scope of the proposed rule to allow for materiality assessments to be communicated within a "reasonably practicable" timeframe[5] for information resources used but not owned by a registrant. Registrants may also need time to design a comprehensive framework and implement robust processes around third-party relationships to allow materiality determinations and any required incident reporting to occur in accordance with the proposed rule. Therefore, while registrants work through such implementation challenges, we recommend that the Commission provide a temporary safe harbor that would limit the liability of registrants to making a reasonable effort to obtain and evaluate information from any impacted third-party information resource when evaluating the materiality of cybersecurity incidents.

Disclosure of Cybersecurity Incidents that Have Become Material in the Aggregate

We support the Commission's decision to require disclosure on Form 10-Q or Form 10-K, as opposed to on Form 8-K, when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate. However, there may be challenges in operationalizing the proposed disclosure requirement as written. For example, determining what constitutes a "series" of incidents may prove challenging due to the complexity and potential number of incidents to evaluate. Furthermore, without clarification, we expect diversity in practice to emerge in interpreting the meaning of "series" and determining the period over which related[6] incidents must be aggregated.[7] To mitigate these challenges, we recommend clarifying the meaning of "series" and limiting the period over which registrants are expected to track a series of incidents to a reasonable period. We also recommend that the Commission

[5] As outlined in the proposed Instructions to Item 1.05 on page 127 of the proposing release.
[6] Page 33 of the proposing release includes a statement that registrants would need to "analyze related cybersecurity incidents for materiality."
[7] Page 34 of the proposing release includes an example in which "a number of smaller but continuous cyber-attacks related in time and form against the same company" are aggregated, but it is unclear over what period registrants would continue to aggregate such attacks.

conduct further field testing to determine whether a clarified definition of "series" would be consistently interpreted and could be effectively operationalized by registrants. We believe more effort in this regard will ultimately yield more comparable and decision-useful disclosure for investors.

Conclusion

We appreciate this opportunity to provide feedback on the Commission's proposed rule on cybersecurity risk management, strategy, governance, and incident disclosure. We thank the Commission for its consideration of our comments and welcome further discussion at your convenience.

Sincerely,

Rudolf Bless

Rudolf Bless
Chair, Committee on Corporate Reporting
Financial Executives International