Crowe LLP
Independent Member Crowe Global

225 West Wacker Drive, Suite 2600
Chicago, Illinois 60606-1224
Tel +1 312 899 7000
Fax +1 312 899 5300
www.crowe.com

May 9, 2022

Office of the Secretary
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-1090

Re: Proposed Rule, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," File No. S7-09-22

Dear Office of the Secretary:

Crowe LLP appreciates the opportunity to provide input on the Securities and Exchange Commission (SEC or Commission) proposed rule, "*Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*" (Proposal or Proposed Rule). In relation to cybersecurity, our services include audits, for which we are required to consider the effects of information technology on financial statements and attestation engagements over controls at service organizations. It is through this lens we provide our comments.

Summary

Our views are organized around the SEC's tri-partite mission of maintaining fair, orderly, and efficient markets, investor protection, and capital formation. In addition, our comments are generally grounded in the following views:

- We agree with the Proposal that "cybersecurity risks and incidents can impact the financial performance or position of a company," and we support the SEC's efforts to provide material information to users with respect to cybersecurity.

- Users and preparers might both, in certain circumstances, benefit from:
  - definitional clarity;
  - additional guidance; or
  - modifications to the Proposed Rule

Maintaining fair, orderly, and efficient markets

Definitional clarity
Proposed Item 106 of Regulation S-K defines three terms: cybersecurity incident, cybersecurity threat, and information systems. However, those definitions might not completely match the definitions commonly used in cybersecurity today, which are drawn from the U.S. Department of Commerce's *National Institute of Standards and Technology* (NIST). NIST provides, though its Information Technology Laboratory, a glossary[1] (Glossary) of terms commonly understood in the context of cybersecurity. The Commission might consider whether it could enhance preparers' ability to consistently apply the Proposal's requirements and provide material disclosures to users by clarifying certain aspects of the proposed definitions or directly

[1] https://csrc.nist.gov/glossary/

referencing the Glossary to assist all entities in applying any final rule in a consistent manner. The SEC might also need to consider pointing to specific definitions within the Glossary when such terms have multiple definitions (for example, the term "cybersecurity" itself has multiple definitions).

The Proposed Rule's definitions of "cybersecurity incident" and "cybersecurity threat" might lead to inconsistent application, and the SEC might consider how the definitions could be enhanced, including by referencing specific Glossary definitions. The Proposed Rule's definitions of "cybersecurity incident" and "cybersecurity threat" include reference to "***any*** information residing" [emphasis added] within a registrant's information systems, including both owned and used systems. The scope of "any" information is quite broad. In contrast, the Glossary definitions of similar terms do not refer to "any" information; rather, the Glossary definitions include qualifiers specifying the type of information intended to be within the scope of the definition.

Broad definitions might cause preparers to incur significant costs assessing cybersecurity incidents that do not result in the need for disclosure. For example, consider a cybersecurity incident involving bank wire instructions. If a bank received fraudulent wire instructions from a mortgage title company, it is unclear whether this is a cybersecurity incident that should be analyzed for possible disclosure under the Proposal. The Commission might consider how the proposed definitions could be enhanced to more clearly identify the types of information impacted by a cybersecurity incident (for example, personally identifiable information, non-public, confidential) that should be analyzed for disclosure.

Auditors also have an interest in having clear and consistent definitions, particularly in situations where the Proposal requires disclosure in a document containing audited financial statements. Under professional standards,[2] auditors are required to read the other information in documents containing the audited financial statements and consider whether such information or the manner of its presentation is materially inconsistent with information appearing in the audited financial statements or contains a material misstatement of fact. To the extent disclosure of cybersecurity incidents appears in a document with audited financial statements, the ability of auditors to comply with professional standards would be enhanced through consistently understood and applied definitions.

Disclosure timing considerations

Timely disclosure of material cybersecurity incidents is key to fair, orderly, and efficient markets and to investor protection. Proposed Item 105 of Form 8-K requires disclosure within four days of the determination that a cybersecurity incident is material. Further, proposed Item 105 requires a registrant to make cybersecurity incident materiality determinations "as soon as reasonably practicable after discovery of the incident." The Proposal notes that materiality determinations might coincide with the date of discovery or might come after, but in any event, the Commission "expect[s] registrants to be diligent in making a materiality determination in as prompt a manner as feasible."

Cybersecurity incidents are typically complex and come in a variety of forms that continually evolve. In our experience, it is very rare for a registrant to be able to make a well-reasoned, objective materiality conclusion on the date of discovery. It can take significant time and effort to investigate, analyze, and conclude on the materiality of a cybersecurity incident after discovery, which necessarily impacts the timing of the relevant disclosure. In certain circumstances where a breach could be material, registrants, as part of a robust investigation process, might hire external parties to perform an investigation of a specific breach, which can take significant time to finalize and reach conclusions. It is unclear how a registrant should interpret "as prompt a manner as feasible" in this circumstance. .

In certain circumstances, the ability to obtain sufficient information to evaluate materiality might be outside the control of the registrant. As noted in the Proposal, a registrant might use third-party information systems through a subscription or license agreement. While such agreements often have contractual

[2] PCAOB Auditing Standard 2710

terms that require the service provider to disclose cybersecurity incidents to its customers, in our experience, it can sometimes be a lengthy process to obtain from third-party providers sufficient information to make a cybersecurity materiality determination given the number of datapoints that might impact the total mix of information that are only available to the third-party provider.

Premature disclosure of a cybersecurity incident prior to obtaining all facts that could influence the total mix of information can have significant negative consequences for registrants, and the Commission might also consider, in the context of prompt disclosure, how best to balance the need for a full investigation of the facts. The Commission might accomplish this balance through providing a principles-based framework to evaluate whether disclosure would be considered "prompt" under the Proposal. We do not believe prescriptive examples on "prompt" would be useful; however, providing examples of how any principles-based framework should be applied would be helpful.

XBRL
The proposed rule requires Inline XBRL tagging of cybersecurity disclosures, which we believe is appropriate and consistent with the Commission's goal to provide readily available and easily accessible information to stakeholders.

Investor Protection

Cybersecurity governance
The Proposal adds Item 407(j) of Regulation S-K, which requires disclosure of any cybersecurity expertise of members of the board of directors, including the nature of the cybersecurity expertise (for example, prior work experience, specific cybersecurity knowledge or skills, or a degree or certification in cybersecurity), and the name of the board member with that expertise. The Proposal points out the *2019-2020 NACD Public Company Governance Survey*[3] concludes cybersecurity is a top board of director priority and cybersecurity incidents and other risks are viewed one of the largest threats to entities. The Proposal suggests these datapoints might mean investors view disclosure of whether any board members have cybersecurity expertise to be important information for investment and voting decisions.

Investor feedback on the relevance of disclosures related to cybersecurity expert representation on boards is important. It is not clear how an investor might interpret an entity's lack of disclosure of a board level cybersecurity expert, but the *NACD Cyber-risk Oversight Handbook 2020*[4] (Handbook) observes "there simply are not enough "cyber experts" to populate every board." The Handbook also raises several questions it recommends boards consider before appointing a cybersecurity expert. The *NACD's Governing Digital Transformation: A Practical Guide*[5] similarly points out that a common pitfall of recruiting "digital directors" is focusing solely on individuals with technical backgrounds because other skills and backgrounds might be more useful from a governance perspective. Thus, whether a board includes a cybersecurity expert might not be as relevant as the other proposed disclosures related to cybersecurity governance (for example, proposed Item 106(c) of Regulation S-K). The SEC might instead consider revising the Proposal to elicit disclosure of how or whether the board engages with experts to execute its governance role over cybersecurity. Such a disclosure would complement the proposed disclosures in Item 106(c) while providing registrants with the flexibility needed to craft cybersecurity governance appropriate to their organization.

[3] https://corpgov.law.harvard.edu/wp-content/uploads/2020/01/2019-2020-Public-Company-Survey.pdf
[4] https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298
[5] https://www.nacdonline.org/insights/publications.cfm?ItemNumber=65983

Aggregation of immaterial events
Proposed Item 106(d)(2) of Regulation S-K requires aggregation of immaterial cybersecurity events and requires disclosure of those immaterial events when material in the aggregate. Users and preparers might benefit from additional clarification of how the aggregation should be performed and what period should be considered for aggregation.

The Proposal provides an example of aggregation stating that a disclosure obligation might be triggered when "one malicious actor engages in a number of smaller but continuous cyber-attacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material, or both." The Proposal also acknowledges that "such incidents conceptually could take a variety of forms," but it is unclear how a registrant should evaluate aggregation. For example, a registrant might interpret the Proposal as requiring aggregation when there is a single actor engaging in multiple attacks. Another registrant might interpret the aggregation requirement as multiple actors engaging in a cluster of similar attacks (for example, multiple intrusions related to hacks of online bank accounts). Other registrants might interpret the aggregation requirement in a different way. It might be useful for the Commission to provide a principles-based framework to evaluate the aggregation of cybersecurity incidents to foster consistent and comparable disclosures across registrants.

The Commission might also consider specifying the relevant timeframe for aggregation, which would also foster consistent and comparable disclosure. The Proposal requires a registrant to disclose in its next periodic report cybersecurity incidents that become material in the aggregate. However, the Proposal does not specify whether the registrant should evaluate those cybersecurity incidents that have occurred since its most recent periodic report, its most recent annual report, its initial registration, or some other period. Further, should additional immaterial cybersecurity incidents occur after the disclosure of incidents that become material in the aggregate, the Proposal does not specify if a new aggregation analysis should begin or if the new incidents should be aggregated with the previously disclosed aggregated incidents. Preparers and users might both benefit from additional clarity on how the Commission expects such analyses to be performed.

Disclosure updates
Proposed Item 106(d) specifies a registrant must provide in its next periodic report any material updates to disclosures made pursuant to proposed Item 105 of Form 8-K. However, proposed Item 106(d)(2) does not appear to contain a similar update requirement for immaterial cybersecurity incidents concluded to be material in the aggregate. Preparers and users might benefit from additional clarity on whether the Commission expects updated disclosure for incidents disclosed pursuant to Item 106(d)(2).

Capital Formation

Potential costs and benefits
The Proposed Rule acknowledges certain costs of additional disclosures. However, the Proposed Rule also posits that registrants might benefit through potential lower costs of capital, and investors and related stakeholders might benefit through reduction of information asymmetries, thereby reducing securities mispricing, as well as lower costs due to more uniform and comparable disclosures. The Proposed Rule also states the Commission is unable to quantify the potential benefits due to various circumstances. We agree with the Commission's perspective that "a rule's potential benefits and costs should be considered in making a reasoned determination that adopting a rule is in the public interest."[6] We encourage the Commission to re-evaluate, after an appropriate passage of time following the effective date of any final rule, the potential costs and benefits with empirical data to determine whether the objective is being achieved.

[6] https://www.sec.gov/divisions/riskfin/rsfi_guidance_econ_analy_secrulemaking.pdf

Closing

We thank the SEC for providing the opportunity to express our views on questions raised in the Request. Please contact Mark Shannon at 202-779-9921 or Sean Katzenberger at 317-208-2426 to answer any questions that the staff might have regarding the views expressed in this letter.

Sincerely,

Crowe LLP

Crowe LLP