AMERICAN BAR ASSOCIATION
Business Law Section

321 N. Clark Street
Chicago, IL 60654-7598
T: 312-988-5588 | F: 312-988-5578
businesslaw@americanbar.org
ababusinesslaw.org

Via Electronic Submission

July 20, 2022

Ms. Vanessa A. Countryman
Secretary
United States Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-1090

Re: File No. S7-09-22
Release Nos. 33-11038; 34-94382
Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Ms. Countryman:

This letter is submitted on behalf of the Federal Regulation of Securities Committee (the "**Committee**" or "**we**") of the Business Law Section of the American Bar Association (the "**ABA**"), on the above-referenced proposing release issued by the Securities and Exchange Commission (the "**Commission**") regarding the proposed amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 (the "**Proposing Release**").[1] We appreciate the opportunity to comment on the proposals.

The comments expressed in this letter represent the views of the Committee only and have not been approved by the ABA's House of Delegates or Board of Governors and, therefore, do not represent the official position of the ABA. In addition, this letter does not represent the official position of the Business Law Section of the ABA nor does it necessarily reflect the views of all members of the Committee.

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release No. 34-94382 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

Recommendations

Incident Reporting on Form 8-K

Timing Considerations

Form 8-K disclosure should not be required until there is something meaningful to disclose. While the Committee is supportive of the Commission's focus on materiality with regard to reporting of cybersecurity incidents, we believe a Form 8-K reporting obligation that is triggered by a materiality determination alone will not result in meaningful, accurate disclosures, while presenting significant challenges for companies that have experienced a cybersecurity incident, including by putting the company at significant additional risk.

Investors only benefit when there is decision-useful information that can be provided. Immediately following the initial discovery of a cyber incident, there is often a dearth of accurate information and much of what is believed to be true at the start quickly turns out to be incorrect as additional facts come to light. Premature disclosure will cause investors more harm than good because they will be making decisions based on information that is often incomplete or inaccurate and without the full context of updated disclosures of other aspects of the company's operations. The adopting release even acknowledges that a company's disclosure about an incident may "lack the precision needed for investors and the market to properly value the securities, potentially leading to information uncertainty, investor under or overreaction to certain disclosures, and thereby mispricing of registrants' securities."

Premature disclosure would also increase the risk of additional attacks and could worsen the incident being reported because the Form 8-K trigger (as proposed, a determination of materiality) will almost always occur before remediation which could lead the threat actor to increase, or other threat actors to initiate, efforts to exploit the existing vulnerability while the opportunity still exists. When the incident relates to a widely-used third-party system, requiring individual companies that use that system to make disclosure, before any disclosure is made by the third-party system provider, acknowledging they are affected will increase the likelihood that a threat actor will seek to exploit the vulnerability. Absent this disclosure, potential threat actors (whether the original threat actor or a different threat actor) may not know the identity of the third-party's customers. This disclosure will create additional risk of the company being attacked.

As noted, Form 8-K incident reporting should only be required when the company is able to make meaningful disclosure and should not be rushed. As an

alternative to requiring the Form 8-K filing within four business days after the company determines that it has experienced a material cybersecurity incident, we believe it would be more appropriate to require Form 8-K reporting when a company determines that it has an obligation under applicable law to notify persons outside the company who are not subject to a confidentiality obligation or when a company voluntarily elects to make a public disclosure – in each case if, and only if, the company has made a determination that the cybersecurity incident at issue is material. As is the case with other Form 8-K triggers requiring a materiality determination (e.g., current Items 2.05 and 2.06), the rules should provide that the trigger occurs when the board of directors, a committee of the board of directors or an officer authorized to do so makes the materiality determination.

Further, neither proposed Item 1.05 nor the Instructions should attempt to rush a company into making the materiality determination right after an incident has occurred and before it is likely to possess sufficient information to draft meaningful disclosure. Therefore, we do not believe the language in the proposed Instructions to Item 1.05 that the materiality determination shall be made "as soon as reasonably practical after discovery of the incident" is necessary and could result in companies making premature and potentially inaccurate disclosures. The inclusion of such an instruction would put pressure on a company to draw conclusions about materiality in the immediate aftermath of an incident with incomplete information in order to avoid any claim that the company could or should have known that the incident was material sooner.

In addition, the timeframe for disclosing third-party incidents should be longer than the timeline for disclosing company incidents given the difficulties a company will face in obtaining relevant information from the third-party provider. The company will need to obtain information from the third-party, and the timing of receiving this information will likely be outside the control of the company. In instances where the third party is not itself a reporting company and/or does not view the incident as material, information flow may be slow, at best. The company also may need time to verify or follow up on information provided, so the process of obtaining information needed to draft accurate and useful disclosure will in many instances fall well outside the four-day trigger for disclosure.

Law Enforcement Exception

Any new disclosure requirement also should include a broad law enforcement exception that applies not only in the interest of national security but also when law enforcement believes disclosure will hinder their efforts to identify or capture the threat actor. The use of a law enforcement or national security exception should be based on discussions with any appropriate governmental agency and not be limited to the Attorney General's office.

Definition of "Cybersecurity Incident"

We note that the definition of "cybersecurity incident" under the proposal is too broad. Under the proposal, a cybersecurity incident is "an unauthorized occurrence on or conducted through an issuer's information system that jeopardizes" the company's information systems. All types of situations could be viewed as "jeopardizing information systems," thus capturing numerous risks that do not actually result in harm to the company. Further, "information systems" is defined as:

> [I]nformation resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

This definition is an overbroad term that could capture anything ranging from a third-party service provider to a company's filing cabinet and would result in significant uncertainty for companies seeking to comply with the new disclosure requirement and, potentially, disclosure that is beyond the scope of what would be useful to investors. Accordingly, we strongly urge that the Commission provide a more tailored and narrow definition that, at a minimum, would require that the information system be within the control of the company. More broadly, and as discussed further below, any new rules should include definitions that are consistent with existing definitions used under other federal laws and regulations, to the extent a comparable definition is available.

Required Disclosures

While we acknowledge that proposed Item 1.05(a) would only require disclosure of information "to the extent known to the registrant at the time of filing", the proposed requirements to disclose "Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose" and "The effect of the incident on the registrant's operations" are nevertheless too detailed given the short timeframe involved and the fact that the company will first apply its resources to ending the event and then commence conducting its initial investigation of the incident. Disclosure of what the company believes it is aware of at the time of initial filing will often ultimately prove to be inaccurate or incomplete and will result in the disclosure of information that is not decision-useful while at the same time unnecessarily exposing the company to disclosure liability claims.

In addition, proposed item (5) ("Whether the registrant has remediated or is currently remediating the incident.") seems unnecessary given proposed item

(1) ("When the incident was discovered and whether it is ongoing"). Alternatively, the phrase "and whether it is ongoing" could be deleted from item (1).

Finally, given the constantly evolving nature of cybersecurity threats, any attempt to list examples of what may be covered will quickly become dated and cease to be helpful.

Application of Safe Harbors and Other Relief

As is the case with other Form 8-K items that require a company to quickly assess the materiality of an event or to determine whether a disclosure obligation has been triggered, any required disclosure regarding a cybersecurity incident should have the benefit of the safe harbors from liability and should not impact a company's ability to use short-form registration statements. We therefore support the Commission's proposed approach in this regard.

Updates to Previous Disclosure Regarding Material Cybersecurity Incidents

To the extent there will be a specific requirement to disclose material changes, additions, or updates to information previously reported regarding a material cybersecurity incident, we believe the appropriate means of disclosing that information, consistent with proposed Regulation S-K Item 106(d)(1), is through disclosure in Forms 10-K and 10-Q rather than Form 8-K. The concept of Form 8-K is that there are certain matters that are so material that a current disclosure is required in advance of the registrant's next periodic report. But the Commission has never imposed a requirement that a registrant effectively provide "live" continuous disclosure about a matter through multiple updating Form 8-Ks, presumably due to Commission efforts to balance registrant burdens and investor benefits of such an approach. Imposing a requirement that registrants continuously analyze potential Form 8-K triggers for a previously disclosed incident would be unprecedented and inconsistent with the Commission's approach to similar serious events, such as material impairments and material financial restatements. Consistent with other Form 8-K triggers, registrants should be able to determine, based on (i) existing applicable law (e.g., duty to update or duty to correct, as applicable), (ii) factual developments subsequent to the filing of the Form 8-K and (iii) other considerations, such as the registrant's capital markets activity, whether further disclosure about a previously reported cybersecurity incident is warranted prior to the next Form 10-K or 10-Q.

Disclosure of Cybersecurity Incidents that Have Become Material in the Aggregate

We do not support proposed Regulation S-K Item 106(d)(2), which would require a registrant to provide disclosure when a series of previously undisclosed

and individually immaterial cybersecurity incidents becomes material in the aggregate. While the Commission may conclude that the sudden and dramatic impact a material cybersecurity incident can have on a registrant warrants adding a specific disclosure item requirement for a material cybersecurity incident, the Commission should continue to rely on existing item requirements for disclosure about the impact of immaterial cybersecurity incidents which, over time, may be material. These other item requirements, which the Commission highlighted in its February 2018 interpretive guidance ("Commission Statement and Guidance on Public Company Cybersecurity Disclosures"), include risk factors, MD&A, legal proceedings, description of business, and financial statements (including contingent liabilities). We do not see a basis for differentiating cumulative cybersecurity incidents from all other matters that could cumulatively impact a registrant, including cumulative legal matters, changes in capital resources, supply chain issues, etc.

If the Commission decides to require disclosure of a series of individually immaterial cybersecurity incidents that become material in the aggregate, the Commission should revise the rule text set forth in the Proposing Release to address the following issues.

First, while the Proposing Release makes clear that the rule is intended to capture a series of *related* incidents[2], the word "related" is not in the text of proposed Item 106(d)(2) and should be added.

Second, the Commission should define "related" in the text of the rule, similar to the way the Commission has in Rule 3-05 and Rule 3-14 of Regulation S-X. We recommend that "related" be defined as cybersecurity incidents that are known by the registrant to have been performed by the same malicious actor or that exploited the same registrant vulnerability.

Third, proposed Item 106(d)(2) should be revised to state that the period for aggregation should run from the end of the registrant's last fiscal year. Again, this is consistent with how the Commission handles aggregation of related individually immaterial events in Rule 3-05 and Rule 3-14. An indefinite time period would unnecessarily increase the burdens on registrants, complicate the Commission staff's ability to administer the rule, and not result in decision-useful information.

To address the three issues described above, we propose the following revisions to proposed Item 106(d)(2):

[2] Page 33 of the Proposing Release states "registrants would need to analyze *related* cybersecurity incidents for materiality…"

> "(2) The registrant should provide the following disclosure to the extent known to management when a series of related previously undisclosed individually immaterial cybersecurity incidents has occurred since the end of the registrant's last fiscal year for which audited financial statements have been filed that are material in the aggregate. "Related" for purposes of this paragraph means cybersecurity incidents that are known by the registrant to have been performed by the same malicious actor or that exploited the same vulnerability;"

Further, the disclosure required by proposed Item 106(d)(2) should be limited to the cumulative impact on the registrant and should not require detailed information about the individual incidents. To avoid burdening registrants and investors with detailed information about incidents which are by definition individually not material, the required disclosure should be limited to a brief description of the nature and scope of the related incidents and the cumulative effect of those incidents on the registrant's operations.

If the Commission decides to require disclosure of individually immaterial cybersecurity incidents that become material in the aggregate, such disclosure should be required in a periodic report rather than a Form 8-K. As noted above, the cumulative impacts of cybersecurity incidents over time are analogous to other matters that cumulatively impact a registrant, like legal matters, liquidity and operational challenges. These types of cumulative impacts are best addressed in periodic reports, in the context of complete information about a registrant's most recent reporting period, and do not necessitate or warrant current disclosure on Form 8-K.

Form 10-K Cybersecurity Policies and Procedures Disclosure

Proposed Item 106(a) – Definitions

The Commission proposes Regulation S-K Item 106(a) to adopt definitions for "cybersecurity incident," "cybersecurity threat," and "information systems." The Committee supports the inclusion of definitions for these terms but believes that these definitions should be consistent with existing definitions used under other federal laws and regulations, to the extent a comparable definition is available. For example, the National Institute of Standards and Technology (NIST) includes the following definition for "cybersecurity" in NIST Special Publication 800-37, Appendix B: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." Aligning definitions with those in existing federal laws and regulations would help ensure that the defined terms are consistently understood, interpreted and applied in the relevant disclosure.

Proposed Items 106(b) and 106(c) – Risk, Strategy and Governance

The Commission proposes Regulation S-K Item 106(b) and 106(c) to require disclosure regarding a company's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board's oversight of cybersecurity risks on Form 10-K. While the Committee generally supports enhancing cybersecurity policies and procedures disclosure, such disclosure only benefits investors when it provides decision-useful information. The proposed scope of Items 106(b) and 106(c) far exceeds the scope of information that would provide investors with decision-useful information, and further, could undermine companies' cybersecurity efforts by providing a detailed roadmap for threat actors seeking to exploit cyber vulnerabilities.

(i) Proposed Item 106(b)

Proposed Regulation S-K Item 106(b) would require companies to disclose detailed information about their policies and procedures to identify and manage cybersecurity risks and threats. Such disclosure would need to include, among other things, information about cybersecurity risk oversight of third-party service providers, previous cybersecurity incidents and cybersecurity risks that are reasonably likely to affect the company's results of operations or financial condition.

Requiring companies to disclose details about third-party entities involved in assessments and audits would be cumbersome and impose a disproportionate

burden, particularly given that many large companies regularly rotate retained firms. Furthermore, certain software service provider information required by the proposed rule may not be obtainable by the company. To the extent disclosure about use and oversight of third parties is required, such disclosure should not require naming the specific third party used, as providing such information would likely increase the risk of cyber-attacks. Similarly, requiring the disclosure of previous cybersecurity incidents and cybersecurity risks reasonably likely to affect the company's results of operations and financial condition would provide threat actors with information about the company's specific cybersecurity vulnerabilities and enable the exploitation of the previous or current vulnerabilities identified. Moreover, the details about a company's incident response and remediation process and techniques (including specific tools and third parties used) is highly sensitive information and could easily be used by attackers to target a company and disable key members of the team. In response to the Commission's request for comment and for the same reasons discussed herein, requiring affirmative disclosure that a company does not have any cybersecurity policies and procedures in place could invite a cyber-attack from a threat actor seeking to identify companies with cybersecurity vulnerabilities. The interest in providing investors with affirmative disclosure is outweighed by the interest in ensuring that such disclosures do not lead to targeted cyber-attacks. In light of these considerations, we support the narrowing of proposed Item 106(b) to require only the disclosure of material policies and procedures, with materiality defined consistently with *TSC Industries,*[3] *Inc. v. Northway, Inc.*, *Basic, Inc. v. Levinson*[4] and *Matrixx Initiatives, Inc. v. Siracusano*.[5]

(ii) Proposed Item 106(c)

Proposed Regulation S-K Item 106(c) would require companies to disclose detailed information related to cybersecurity governance, including the board's oversight of cybersecurity risks and a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of such management, and its role in implementing the company's cybersecurity policies, procedures and strategies.

The Committee believes proposed Item 106(c) requires disclosures that are far too granular and would result in over-disclosure that would obfuscate material information regarding a company's cybersecurity risk governance amidst a barrage of information, such as the frequency of management reports to the board and the details of internal processes for communicating, preventing, monitoring, detecting and remediating cybersecurity incidents. We believe such detailed disclosure requirements are not warranted, and in addition to running the risk of burying decision-useful information, would also result in companies

[3] TSC Indus. v. Northway, 426 U.S. 438, 449 (1976).
[4] Basic Inc. v. Levinson, 485 U.S. 224, 232 (1988).
[5] 563 U.S. 27 (2011).

issuing boilerplate and immaterial disclosures. Additionally, we note that companies have varied structures and processes for managing and overseeing cybersecurity risk, but that the specifics of such structures or processes does not necessarily reflect the companyies' cybersecurity maturity or sophistication. There is great potential for investors to draw the wrong conclusions about the effectiveness of a company's cybersecurity defenses based on a comparison of these disclosures across companies. Finally, we do not see a rationale for requiring such vastly different and more detailed disclosures regarding a company's cybersecurity risks in comparison to all other risks a company manages and oversees. For some companies (e.g., those where information technology or data-collection represents a material portion of the business), cybersecurity is a principal risk that may require more attention and oversight than other risks. However, for other companies (e.g., those where electronic information collection or storage is incidental to the business), there may be other risks that pose significantly greater threats to the company. Given this variance and the multitude of risks faced by most companies, proposed Item 106(c) disclosures should be revised to require only a high-level explanation of management's and the board's role in cybersecurity risk management and oversight in a manner that situates cybersecurity risk disclosures among and on par with other risks a company may face.

In response to the Commission's request for comment, we believe that Item 106(c)(1) should instead be adopted under Item 407, which would result in the board oversight disclosure being included in the proxy statement alongside Item 407(j) and other corporate governance disclosures. The proposed Item 106(c)(1) disclosure relates to corporate governance and board oversight topics covered in Item 407 and required in the proxy statement, which would be the logical place that investors would look to for disclosure regarding board oversight of cybersecurity and cybersecurity risk.

Form 10-K and Proxy Statement Board Expertise Disclosure

Proposed Item 407(j)

The Commission proposes Regulation S-K Item 407(j) to require disclosure in a company's Form 10-K and proxy statement about the cybersecurity expertise of any members of the board of directors. The Committee believes that a board's role in risk oversight, including cybersecurity risk oversight, does not require members of the board to have specific expertise in cybersecurity. Companies retain and benefit from employees or advisors with the cybersecurity expertise to manage and advise on highly technical cybersecurity topics or areas of concern applicable to the company and its industry. The board's role is to oversee an ever-changing range of risks confronting a company, which requires broad-based skills in risk and management oversight, rather than subject matter expertise in one particular type of risk. Consequently, requiring

specific disclosure regarding a director's expertise in cybersecurity may have the unintended effect of boards de facto delegating cybersecurity risk oversight to the identified individual(s) and reducing the board's sense of collective responsibility for cybersecurity risk oversight. There is also great potential for investors to draw the wrong conclusion about the effectiveness of a board's oversight of cybersecurity based on the identification (or not) of a director with cybersecurity expertise.

However, if the Commission nevertheless proceeds with the adoption of Item 407(j), the definition of "expertise" should be broadly defined to match how companies disclose other skills in the annual proxy statement. The Committee proposes the following revisions to the proposed rule:

> (j) Cybersecurity expertise or experience. (1) If any member of the registrant's board of directors has expertise or experience relating to cybersecurity, disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise or experience. In determining whether a director has expertise or experience relating to cybersecurity, the registrant's board of directors should consider, among other things factors it deems relevant:

We believe that the above revision would capture a broader range of skill sets related to cybersecurity risk management and expertise. The term "expertise" currently appears to capture only those individuals with experience or a prior role singularly focused on information security, while the term "experience" would allow boards of directors to identify and disclose the relevant skills of those directors with prior experience in a broader range of related fields (e.g., those with experiences as Chief Technology Officers, Chief Information Officers or in data privacy roles). Unlike the "audit committee financial expert" disclosure requirement in Item 407, which includes a set of objective criteria (e.g., an understanding of generally accepted accounting principles and financial statements) that can be assessed through the completion of annual director questionnaires, the term "expertise" here does not have sufficiently objective criteria that would allow companies to assess whether a director fulfills the qualification. Just as the scope of "cybersecurity" is broad, the range of skills and experiences potentially relevant to the oversight of cybersecurity is also broad. Proposed Item 407(j) should be revised to ensure that those with relevant cybersecurity skill sets and experiences qualify as having such under the rule.

Finally, we believe the proposed Item 407(j)(2) safe harbor should be adopted to clarify that a director identified as having expertise in cybersecurity would not have any increased level of liability under the federal securities laws as a result of such identification. The absence of such safe harbor could result in prospective directors with cybersecurity expertise being reluctant to serve on boards of directors.

* * *

We appreciate the opportunity to participate in this process and respectfully request that the Commission consider our recommendations and suggestions. We are available to meet and discuss these comments or any questions the Commission and its staff may have, which may be directed to the individuals listed below.

Very truly yours,

Jay H. Knight
Chair of the Federal Regulation of
Securities Committee

Drafting Committee:

Lillian Brown, Chair
John Beckman
Brian V. Breheny
Eric T. Juergens
Stanley Keller
Khadija Lalani
William McComas
Michael McTiernan
Paul Monsour
Brendan Oldham
Jonathan Wolfman

33303174.4