Davis Polk

Davis Polk & Wardwell LLP
450 Lexington Avenue
New York, NY 10017
davispolk.com

May 6, 2022

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
Release Nos. 33-11038; 34-94282
File No. S7-09-22

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington D.C. 20549-1090

Dear Ms. Countryman:

We are submitting this letter in response to the Commission's request for comments on its Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proposal (the "**Proposal**")[1]. As our comments address only certain aspects of the Proposal, we have arranged them by topic rather than by question number.

Reporting of Cybersecurity Incidents on Form 8-K

The Proposal anticipates that the proposed Form 8-K reporting requirement would result in more informative and more timely disclosure than is currently the case[2]. Moreover, though acknowledging that disclosure of such incidents in a Form 10-K or Form 10-Q "would allow for more time to assess the financial impact of such incidents" and the "resulting disclosure might be more specific or informative", the Proposal rejects this option as "it would lead to less timely reporting on material cybersecurity incidents."[3] As such, the Proposal favors immediate reporting of information that is potentially less useful to investors over reporting of information, even if later in time, that is more useful.

Based on our experience in advising clients that are considering disclosure of a cybersecurity incident, we are concerned that the proposed Form 8-K reporting obligation will lead to the reporting of information that will not be decision-useful to investors. While the Proposal only requires reporting of a cybersecurity incident following a determination that such incident is *material*, we expect that registrants will be inclined to report as soon as possible without the benefit of a considered analysis of the impact of the incident on the registrant in light of all of the relevant facts and circumstances giving rise to the event, which may not be known for some time. Registrants will do this out of a concern that, if judged in hindsight, they will be criticized for not reporting an incident when they thought that it *could* be material, even if they have not yet determined that it *is* material. Moreover, such concern will be exacerbated by the proposed (and unusual) requirement that registrants must "make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."[4] As a result, we believe that registrants will report information of a lesser quality that is not necessarily informative for investors (*e.g.*, basic,

[1] Cybersecurity, Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (proposed Mar. 9, 2022).

[2] *Id.* at 16607.

[3] *Id.* at 16613.

[4] *Id*. at 16596.

immediately known facts), and this could lead to investor confusion and the mispricing of the registrant's securities. The fact that registrants could update their disclosure in subsequent reports (either voluntarily or as a result of the Proposal's requirements) to provide more considered and better information for investors will be cold comfort to those investors who may suffer a loss as a result of the mispricing of the registrant's securities following the initial report.

In contrast, as the Proposal acknowledges, using a Form 10-Q and Form 10-K to disclose cybersecurity incidents would permit registrants more time to collect the relevant facts, consider and analyze a given incident, and provide higher quality, more informative disclosure to investors of material incidents.

Needless to say, as is now the case, the absence of a specific Form 8-K *requirement* does not prevent a registrant from voluntarily disclosing the occurrence of a material cybersecurity incident by way of Form 8-K, or other Regulation FD-compliant method.

Disclosure of a Registrant's Governance Regarding Cybersecurity Risks

Our comments on this aspect of the Proposal proceed from the premise that any new disclosure requirement should seek to deliver material information for investors and not be duplicative of other disclosure requirements. As such, we submit that the proposed new Regulation S-K Item 106(c) is unnecessary because any material information captured by the proposed rule is either already adequately addressed by Item 407(h) of Regulation S-K (in respect of the board's oversight role) or could be addressed with minor revisions to proposed Item 106(b) (in respect of management's role).

As the Commission noted in 2018, pursuant to Regulation S-K, Item 407(h): "A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk."[5] We submit that the proposed Item 106(c)(1) duplicates this requirement, insofar as it relates to material information, and otherwise requires an excessive level of immaterial detail, such as how a board is informed about cybersecurity risks and the frequency of its discussions on this topic.

Regarding the proposed Item 106(c)(2), we submit that adding the topic "the registrant's cybersecurity risk management organization, including management's role in assessing and managing cybersecurity-related risks" to the enumerated list of topics to discuss in Item 106(b) would obviate the need for Item 106(c)(2), thereby removing overlap between proposed 106(c)(2) and Item 106(b).

Disclosure Regarding the Board of Directors' Cybersecurity Expertise

We agree with the Commission[6] that cybersecurity is already among the top priorities of many boards of directors. However, we submit that it does not automatically follow, as the Commission asserts, that investors may therefore find disclosure of whether any board members have cybersecurity expertise to be important. Rather, as with other elements of public company operations and risk management, investors expect the board to exercise oversight of cybersecurity risk management by, among other things, ensuring that management possesses appropriate expertise in the field of cybersecurity, including a suitably credentialed Chief Information Security Officer ("CISO") or similarly situated management expert where appropriate. However, while the board will exercise oversight of that CISO or other designated management as part of its general oversight of cybersecurity risk management, it is management that

[5] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459, 83 Fed. Reg. 8166 (Feb. 26, 2018) at 8170, *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[6] 87 Fed. Reg. at 16601.

applies their expert knowledge day-to-day. The technical background of any specific board member is not inherently relevant to his or her ability to oversee and manage risk, whether that risk is cybersecurity or some other similarly important part of the business.

Moreover, companies balance many important factors when assembling a board of directors, including experience, expertise and diversity. As a result, although many companies have directors who are qualified to assess cybersecurity oversight (and indeed oversight of other important areas), in our experience directors usually do not have the specific technical background that the Proposal seems to envision, such as prior experience as an incident response manager or a certification in cybersecurity. Because many companies today may not have a director who would meet the Proposal's stated expertise criteria (or who would be comfortable being so named), this novel disclosure requirement may impact boards' thinking on composition and refreshment issues at a time when multiple competing priorities are also at play. This would, in our view, be an unfortunate distraction.

Definition of cybersecurity incident

We note that the definition of cybersecurity incident refers to an occurrence that "jeopardizes" the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. We are concerned that this suggests that an occurrence that merely has had the *potential* to cause a harm, including loss of confidentiality, integrity, or availability of a registrant's information systems or any information residing therein, is nonetheless reportable even if no such harm *actually* occurs. Though the examples of cybersecurity incidents provided in the Proposal[7] suggest that there should be a compromise, degradation, interruption, loss of control, theft or other *actual* harmful impact on a registrant's information systems, we nonetheless urge the Commission to revise the definition of cybersecurity incident to make clear that the registrant must experience an *actual* harmful impact before a cybersecurity incident is reportable.

* * *

We appreciate the opportunity to participate in the Commission's rulemaking process, and would be pleased to discuss our comments or any questions that the Commission or its staff may have, which may be directed to John B. Meade, Shane Tintle or Meaghan Kennedy of this firm at [redacted].

Very truly yours,

Davis Polk & Wardwell LLP

[7] *Id*. at 16596.