ASSOCIATION OF THE BAR
OF THE CITY OF NEW YORK

COMMITTEE ON
SECURITIES REGULATION

ROD MILLER

CHAIR
MILBANK LLP
55 HUDSON YARDS
NEW YORK, NY 10001
Phone: (212) 530-5022
RDmiller@milbank.com

EVAN J. CAPPELLI
SECRETARY
MILBANK LLP
55 HUDSON YARDS
NEW YORK, NY 10001
Phone: (212) 530-5632
ECappelli@milbank.com

May 9, 2022

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

Via email to rule-comments@sec.gov

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

Dear Ms. Countryman:

This letter is submitted on behalf of the Securities Regulation Committee of the New York City Bar Association (the "**Committee**"). We are responding to the request of the Securities and Exchange Commission (the "**Commission**") for comment on its proposed rules regarding cybersecurity risk management, strategy, governance and incident disclosure (the "**Proposal**" and, any individual proposed rule, a "**Proposed**" rule).

The Committee includes a wide range of practitioners whose areas of interest and expertise include securities laws and the regulation of the U.S. capital markets and who are employed by or advise public companies, including both domestic and foreign private issuers. The Committee does not represent any client and the views expressed by the Committee are those of the Committee and not necessarily the views of any of its individual members or their respective firms or institutions.

Substantive Recommendations

The Committee has certain concerns regarding the substantive aspects of the Proposal, which are set forth below, along with certain recommendations of the Committee for addressing such concerns.

Requirement to File an Item 1.05 Form 8-K. The Committee respectfully submits that as Proposed, Item 1.05 of Form 8-K imposes potentially undue burdens on registrants at a time (*i.e.*, in the aftermath of discovery of a cybersecurity incident) when: (i) a registrant's information gathering may be negatively affected by the incident itself; (ii) information about the incident available to the registrant may be incomplete or inconclusive; and (iii) a registrant's internal management and compliance resources may be under significant strain. Further, the Items required to be disclosed under current Form 8-K generally: (i) relate to events within a registrant's control; (ii) events with respect to which a registrant has some advance warning or awareness and/or (iii) events that are influenced by a registrant's volitional acts. As such, Proposed Item 1.05 is qualitatively different from the other Items requiring disclosure under Form 8-K, and given the myriad challenges tied to identifying, understanding and managing a cybersecurity incident, the Committee believes that augmented cybersecurity incident disclosure requirements are more appropriately applicable to a registrant's Quarterly Reports on Form 10-Q and Annual Report on Form 10-K. This is particularly true in the Committee's view given the fact that: (i) cybersecurity is a pervasive threat affecting all registrants; (ii) the pervasive nature of this threat and the potential consequences of a cybersecurity incident are well known to the investing public (one need only walk through an airport and take in the advertisements for cybersecurity firms to know how mainstream these issues have become); and (iii) investors are certainly on notice as to a registrant's cybersecurity risks through extant risk factor disclosure practice. The Committee acknowledges the Commission's concern that disclosure practices in this regard vary widely; however, it is the Committee's view that any inadequacies in this regard could be effectively addressed by more comprehensive disclosure requirements applicable to quarterly or annual, rather than current, reports filed under the Securities Exchange Act of 1934, as amended (the "**Exchange Act**"). For the foregoing reasons, the Committee respectfully submits that Proposed Item 1.05 of Form 8-K places a potentially undue burden on a registrant experiencing a cybersecurity incident, and the Commission should not amend Form 8-K to include Proposed Item 1.05.

The Committee also respectfully submits that the ambiguity inherent in Instruction 1 to proposed Item 1.05 will make it difficult for a registrant to determine whether it is compliant with its reporting obligations under Proposed Item 1.05 of Form 8-K. The Committee is also concerned that providing examples of "timeframes that would (or would not), in most circumstances, be considered prompt "will provide a false sense of certainty in the context of highly variable, fluid and uncertain events. Instead, as noted above, the Committee respectfully suggests that Form 8-K not be amended to include Proposed Item 1.05.

To the extent that the Commission adopts Item 1.05 to Form 8-K as proposed, the Committee suggests the following modifications: (i) the requirement to file an Item 1.05 Form 8-K be based not only on the determination by the registrant that it has experienced a material cybersecurity event, but that the filing be required only to the extent that the

information upon which the determination is based has been deemed by the registrant to be (a) verified as accurate with a high degree of confidence and (b) unlikely to materially change and (ii) the filing period within which an Item 1.05 Form 8-K is required to be filed be lengthened by at least one business day (*i.e.*, the Form would be required to be filed within 5 business days or more of the registrant's determination). The Committee believes that these two changes would increase certainty in a registrant's disclosure and more appropriately balance the Commission's objectives of timely disclosure against the burdens on a registrant in the context of a cybersecurity incident.

Proposed Inline XBRL Tagging Requirement. The Committee is also concerned regarding the Proposed Inline XBRL tagging requirement, and specifically, that given the time sensitive nature of the disclosures being made, such Proposed requirement unduly adds to the burden of companies already dealing with a multi-pronged response to a material incident. Accordingly, the Committee respectfully proposes that, to the extent the Proposal is adopted, that the Proposed Inline XBRL tagging requirement not be included.

Proposed Amendments to the Eligibility Provisions of Form S-3 and Form SF-3 and Safe Harbor Provisions in Exchange Act Rules 13a-11 and 15d-11. As noted by the Commission, the purpose of the Proposals is to provide "more timely and consistent disclosure about material cybersecurity incidents." The benefits of providing this information should be weighed in the context of the uncertainties inherent in and the burdens related to the production of disclosures relating to cybersecurity incidents (particularly at or shortly following discovery). As such, should the Commission amend Form 8-K to include Proposed Item 1.05, the Committee believes that the Proposed Amendments to Form S-3 and F-3 and to the Exchange Act safe harbor provisions noted above is appropriate and warranted.

Exception for Cybersecurity Incidents Under Investigation. The Proposal would require a registrant to file an Item 1.05 Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. The Proposal does not provide for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident. In the relevant discussion on point, the Commission recognizes that "a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents." The Committee respectfully suggests that the Commission has not given appropriate weight to the necessity to delay such disclosure in the context of an ongoing investigation (particularly by law enforcement). A delay in reporting may not only facilitate such an investigation, it may be critical to its success. The Committee is concerned that requiring such current disclosure without exception will more likely alert cybercriminals to detection of their infiltration, which could enable them to abscond prior to apprehension or before the relevant methods of infiltration and exfiltration used by the criminals have been analyzed and mapped. This would have the effect of depriving the commercial sector and law enforcement agencies alike of the knowledge base necessary to more effectively address ongoing and future cybersecurity incidents. Further, it is a fact that law enforcement agencies have in the past and may in the future request that a registrant that has experienced a cybersecurity incident keep the fact of the incident confidential for a specified period of time. Without an exception to Proposed Item 1.05 of Form 8-K, a registrant could find itself having to deny such a law enforcement request. Finally, the Committee is concerned that the Proposal includes little discussion or seems to reflect inadequate consideration of the national security implications of current (and potentially premature) disclosure of a

cybersecurity incident under Item 1.05 of Form 8-K as Proposed. A failure to apprehend cybercriminals and fully analyze the relevant methods of infiltration and exfiltration deprives the national security firmament of tools necessary to address constantly evolving cybersecurity threats. The Committee notes that these potential harms to national security from a premature disclosure are at their most severe in the context of a cybersecurity incident at a registrant with government contracts or with a business that is focused on national security matters. The Committee believes that ensuring that these types of registrants are sufficiently able to manage a cybersecurity incident out of the public eye is of significant import.

To address the Committee's concern in this regard and assuming that Form 8-K is amended as Proposed, the Committee recommends the Commission include an exception from the current reporting requirement under Proposed Item 1.05 of Form 8-K when a cybersecurity incident is the subject of a *bona fide* internal investigation or investigation by law enforcement. Any such delayed disclosure should, of course, be required to be made under cover of Form 8-K (or a proximate periodic report if appropriate) as soon as is reasonably practicable. Further, as a means to ensure that registrants utilize such an exemption appropriately, the Commission could require a registrant delaying Form 8-K disclosure of a cybersecurity incident to include the following disclosure in the Item 1.05 Form 8-K disclosure ultimately filed (or, if such disclosure is instead included in a periodic report, that report): (i) confirmation of the fact that the incident was the subject of an investigation and (ii) the basis for utilizing the filing delay.

Definition of "Cybersecurity threat". The definition of "Cybersecurity threat" as Proposed means: "any potential occurrence that *may* result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein." (*emphasis added)*. The Committee respectfully submits that the use of a "may" standard establishes a standard that would require registrants to establish policies and procedures that are potentially overbroad and not appropriately tailored to those threats that are reasonably foreseeable. As such, the Committee suggests that the definition of "Cybersecurity threat" be revised by replacing "may" with "could reasonably be expected to".

* * *

We thank you for the opportunity to comment on this important Commission initiative. Members of our Committee would be happy to discuss any aspect of this letter with the Commission staff.

Respectfully submitted,

_____

ROD MILLER
Chair

Securities Regulation Committee
Association of the Bar of the City of New York