Hope M. Jarkowski
General Counsel
New York Stock Exchange
11 Wall Street
New York, NY 10005
[redacted]

May 9, 2022

Via Email

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

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

Dear Ms. Countryman:

On behalf of NYSE Group, Inc.[1] ("NYSE" or the "Exchange"), we appreciate the opportunity to comment on the U.S. Securities and Exchange Commission ("Commission") proposal to adopt rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies (the "Proposal")[2].

The NYSE is the world's largest exchange, home to more than 2,400 listed companies having an aggregate market capitalization of more than $35 trillion. In this capacity, the Exchange recognizes the critical role that technology plays for companies across all industries and sectors. Given the importance of technology to the business and operations of virtually all listed companies, the Exchange acknowledges that information around an issuer's cybersecurity risk management and incident response may be material to investors.

To that end, the NYSE is generally supportive of the Proposal, but offers the following comments to help ensure that: (i) the Proposal's requirements result in disclosure that is most helpful--rather than overly detailed--to advancing investors' understanding of a company's cybersecurity risk; (ii) smaller and medium sized companies are not unfairly disadvantaged by the Proposal's disclosure requirements around board member cybersecurity expertise; (iii) issuers retain the ability to delay *public* disclosure of an ongoing cybersecurity incident pending remediation of the incident; and (iv) issuers retain the ability to delay *public* disclosure of a cybersecurity incident for active law enforcement investigations, national security, or critical infrastructure protection purposes.

[1] NYSE Group submits this letter on behalf of New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., NYSE Chicago, Inc. and NYSE National, Inc.

[2] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, File No: S7-09-22 (March 9, 2022), 87 FR 16590 (March 23, 2022).

The Proposal's Mandated Disclosure Are Overly Detailed and May Inhibit Companies from Providing Investors with Useful Disclosure About Cybersecurity Risk

The NYSE agrees with Commission's assertion that cybersecurity is among the top priorities of many, if not most, boards of directors. Accordingly, many public companies have already developed robust cybersecurity policies and procedures that enable them to manage risks unique to their businesses and make required disclosures consistent with previous Commission guidance. The NYSE is concerned that the Proposal's disclosure requirements could result in the creation of de facto minimum standards that: (i) constrain management's ability to address cybersecurity risks in a manner most suitable for their business; and (ii) give investors the mistaken impression that companies do not take their duty to mitigate cybersecurity risk seriously.

Proposed Item 106

Proposed Item 106 of Regulation S-K will mandate disclosures around a company's cybersecurity policies and procedures and oversight of cybersecurity risk. Among other things, proposed Item 106 would require companies to disclose: (i) whether they "engage assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;"[3] (ii) "whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks;"[4] (iii) "the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic;"[5] and (iv) "whether the registrant has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart."[6]

The Exchange is concerned that the granular disclosures of organizational minutiae required by proposed Item 106 may result in overly detailed filings that have little utility to investors. By requiring this level of specificity in periodic filings, the Proposal focuses company disclosure on the form--rather than the substance--of management review. When formulating a cybersecurity risk management plan, the Exchange worries that the prescriptive requirements of proposed Item 106 may lead to corporate decision making that is driven in greater part by a desire to fit within perceived norms than by what makes sense organizationally. Accordingly, the Exchange recommends that the Commission reconsider whether all of the required disclosures mandated by proposed Item 106 are necessary or useful to investors.

Proposed amendment to Item 407

The proposed amendment to Item 407 of Regulation S-K raises many of the same concerns discussed above. As amended, Item 407 would require a company to disclose whether any member of its board has expertise in cybersecurity and, if so, describe the nature of that expertise.

Although these proposed amendments do not *mandate* that corporate boards include a member with expertise in cybersecurity, they have the implicit suggestion that corporate boards

[3] See Proposed Item 106(b)(2).
[4] See Proposed Item 106(c)(1)(i).
[5] See Proposed Item 106(c)(1)(ii).
[6] See Proposed Item 106(c)(2)(ii).

should include a member with such qualifications. Failure to have a board member with expertise in cybersecurity, therefore, could result in investors reaching the mistaken conclusion that a company is unconcerned with cybersecurity. While the Exchange agrees with the Commission that cybersecurity is an important area of focus for nearly all public companies, it does not believe that the absence of a cybersecurity expert on a company's board is necessarily the fatal flaw that the required disclosure may implicitly suggest to investors. Corporate boards consider a wide range of important issues and should have broad discretion to determine how they educate themselves on each subject. In the area of cybersecurity, a corporate board may rely on reporting from an in-house cybersecurity team or external consultants. Relying on non-board member experts should not suggest that a company is unserious about cybersecurity.

Further, the Proposal makes clear that there is no uniform set of credentials that constitutes "cybersecurity expertise." Consequently, each public company will determine for itself whether one or more of its board members qualifies as an expert in this complicated and evolving area. The Proposal enumerates criteria that a board may consider in concluding whether one of its members has cybersecurity expertise, but much of the criteria is vague such as having "knowledge…or other background in cybersecurity." The Exchange is concerned that these ambiguous criteria may result in corporate boards reaching inconsistent conclusions about the cybersecurity expertise of their members. The potential for such divergent conclusions increases the likelihood of investor confusion and calls into question the ultimate usefulness of this disclosure at all. Accordingly, the Exchange urges the Commission to remove the proposed amendments to Item 407 from any final rule.

If the Proposal is adopted in its current form, the Exchange believes that many companies will prioritize attracting board members with "cybersecurity expertise" in order to demonstrate their commitment to managing cybersecurity risk. With 7,848 companies filing on domestic forms and 973 FPIs filing on foreign forms during calendar year 2020, the NYSE questions whether there are truly enough individuals with both cybersecurity expertise and other relevant experience to make them suitable candidates for service on a corporate board. If a shortage does exist, the Exchange is also concerned that smaller and medium-sized companies may be disproportionately disadvantaged in attracting these highly sought after individuals for board service.

For the reasons discussed above, the Exchange asks the Commission to reconsider amending Item 407 of Regulation S-K. Currently, information on the business expertise of board members is disclosed pursuant to Item 401(e) of Regulation S-K and the Exchange believes that such disclosures are sufficient to educate investors on the qualifications of a company's board.

The Proposal's Immediate Disclosure Requirements May Interfere with Ongoing Investigations to the Detriment of Investors

Proposed Item 1.05

The Proposal recommends adopting new Item 1.05 of Form 8-K to require companies to publicly disclose information about a material cybersecurity incident within four business days. Notably, proposed Item 1.05 does not allow for any delay in reporting when there is an ongoing internal or external investigation related to the cybersecurity incident. While the Exchange understands the benefit to investors of prompt disclosure, it is concerned that the Proposal's strict four-day reporting requirement may compromise investigations that could lead to the recovery of stolen funds or apprehension of bad actors.

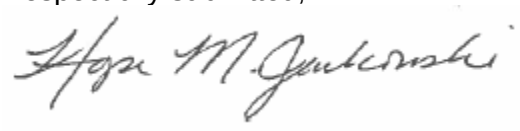
The Exchange believes an issuer should not be compelled to *publicly* disclose information regarding an *ongoing* cybersecurity incident to the detriment of the company's active remediation efforts. Cybersecurity attacks are increasingly complex and can be carried out in several phases. Premature public disclosure of an incident without certainty that the threat has been extinguished could provide bad actors with useful information to expand an attack. Many public companies already have procedures in place to share critical information about a cyber incident with relevant federal law enforcement agencies such as the Federal Bureau of Investigations and the Department of Homeland Security. Recent legislation such as the Cyber Incident Reporting for Critical Infrastructure Act expands this framework to help establish a comprehensive reporting regime for information around a cyber incident. The Exchange believes that public companies should not be burdened with yet another set of public reporting obligations as set forth in the Proposal. In addition to revealing sensitive information while an attack may be ongoing, the Proposal's reporting requirements will strain the resources of many company's cybersecurity teams, all to the detriment of the investing public.

Additionally, as the Proposal notes, many states have laws that allow companies to delay public disclosure of a cybersecurity incident if law enforcement determines that such disclosure will interfere with a civil or criminal investigation. Cybersecurity is a complex and ever-evolving area, and the Exchange believes that public company investors benefit as a whole when cybersecurity intrusions are prevented. To that end, the Exchange believes that, under limited circumstances, the Proposal should provide a safe harbor permitting companies to delay public reporting of a cybersecurity incident if such delay is reasonably likely to lead to the recovery of stolen funds, apprehension of bad actors, or prevention of future cybersecurity incidents.

Conclusion

The NYSE recognizes the importance to public companies of managing cybersecurity risk and is largely supportive of the Commission's efforts to standardize disclosures in this area. As discussed above, the Exchange believes certain aspects of the Proposal's disclosure requirements may be viewed as establishing effective governance minimums and risk burdening companies with excessive reporting requirements that do not correspond to a related benefit to investors. The Exchange also encourages the Commission to carefully consider whether some of the Proposal's requirements may inadvertently inhibit--rather than help--thorough investigations into cybersecurity intrusions to the detriment of retail investors, law enforcement and cybersecurity incident prevention in the future.

Respectfully submitted,



Hope M. Jarkowski
General Counsel, NYSE Group