John A. Zecca
Executive Vice President,
Chief Legal and Regulatory
Officer
805 King Farm Blvd.
Rockville, MD 20850

May 9, 2022

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F. Street NE.
Washington, DC 20549

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

Dear Ms. Countryman:

The Nasdaq Stock Market LLC[1] ("Nasdaq") appreciates the opportunity to comment on a recent proposal by the Securities and Exchange Commission ("Commission") to require current reporting of material cybersecurity incidents 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 "Proposal").[2]

Nasdaq supports the Proposal's goals to enhance and standardize disclosures regarding cybersecurity and agrees that cybersecurity threats pose an ongoing and escalating risk to public companies, investors, and market participants. Requiring public companies to disclose uniform information about cybersecurity risk management, strategy, and governance practices would provide investors with comparable information to assess how public companies manage cybersecurity risk, thereby promoting transparency and consistency. Nasdaq believes that investors, issuers and other market participants will benefit from healthy capital markets that promote trust and transparency.

However, as Nasdaq considered the Proposal in our role as a national securities exchange serving as a listing venue, the Proposal raised some concerns for our listed companies. We received valuable feedback from our issuer community, which includes companies of various

[1] The Nasdaq Stock Market LLC is registered as a national securities exchange and is wholly owned by Nasdaq, Inc.

[2] See Securities Exchange Act Release No. 94382 (March 9, 2022), 87 FR 16590 (March 23, 2022) (File No. S7-05-22) (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure).

sizes and market capitalizations, about issues that are important to them. Nasdaq addresses below certain concerns that are raised by this Proposal for those listed companies.

Time Period For 8-K Disclosure of Cybersecurity Information Is Too Short

Nasdaq received feedback from listed companies concerning the requirement to disclose information about a cybersecurity incident within four business days after the company determines that it has experienced a material cybersecurity incident. The feedback indicated that the four business day timeframe (1) may interfere with a public company's primary obligation to remediate a cybersecurity intrusion; and (2) is an exceptionally short time period in which to understand the nature and scope of a cybersecurity breach as well as its potential impact.

Once a breach of a company's information systems has been discovered, it is paramount for a company to understand the scope and nature of the cybersecurity incident and immediately commence remediation efforts to limit the amount of damage that such an incident may cause. Time is of the essence for a company dealing with a cybersecurity incident. However, the requirements of this Proposal, including the determination of materiality itself, could distract key employees and management away from remediation efforts. In these situations, public companies should be permitted to prioritize first on protecting the company's information systems and averting further damage over other priorities. The feedback we received is that greater flexibility should be provided to public companies with respect to the timeframe to disclose a cybersecurity incident so as not to divert critical efforts away from remediation efforts.

The discovery of a potential breach of a company's information systems would trigger a series of necessary actions to arrive at a determination that a breach was material including, but not limited to, an internal investigation, extensive communication with and oversight from senior management, and the board of directors, together with communication with external parties (outside counsel, advisors, expert consultants and regulators). The four business day timeframe may not provide public companies with adequate time to investigate and formulate next steps much less prepare a fulsome and thorough disclosure and as a result, may hinder a company's investigation into a breach, potentially precluding a deliberate and systematic investigation, which could result in incorrect or incomplete conclusions being drawn early on and being disclosed within the Form 8-K. We believe disclosures that are premature, and potentially incomplete or ultimately misleading, do not further investor protection and do not promote well-functioning orderly and efficient markets. Rather, incomplete or misleading disclosures have the potential to exacerbate the original harm imposed by a bad actor. Hasty disclosures forced by the need to comply with the four business day timeframe could impair both public companies and investors if investments are made based on piece meal information. Nasdaq acknowledges that in some cases more expeditious disclosure may be justified and requests the Commission consider providing some flexibility in the timing of the disclosure to allow public companies the necessary time to prepare and file more informed disclosures.

Finally, public companies bear risk in making materiality determinations in a timely manner where facts and circumstances are fluid, as is the case with cybersecurity incidents. When a material cybersecurity incident is disclosed, there will likely follow questions regarding the company's actions, including the timing of disclosure and materiality determination itself, which could further complicate, and even potentially alter, the company's investigations,

remediations and communications with key stakeholders. In addition, actions taken with best intentions and with information available at the time could, in hindsight, be considered mistakes. Given this risk, Nasdaq suggests the Commission grant a safe harbor to public companies with respect to the timing of reporting and determination of materiality made in good faith. Such protection would allow public companies to conduct methodical investigations and remediations, as well as make disclosures, without the fear of being second-guessed.

Smaller Reporting Companies Should be Permitted Additional Time to Comply

The Proposal would require public companies to disclose policies and procedures to identify and manage cybersecurity risks and threats, including, operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk.[3] As a result, public companies would need to review and adopt expanded governance policies to meet the required disclosures. Also, because a cybersecurity incident refers to "any information"[4] residing in a company's information systems, the Proposal would impact the manner in which a public company reviews and retains data over an unlimited time period since a public company would need to necessarily monitor all incidents, whether material or not. Further, in light of the Proposal, public companies may need to attract suitably qualified individuals with cybersecurity expertise. These additional requirements may disproportionately impact smaller reporting companies with fewer resources and, as such, Nasdaq believes that the Commission should provide a longer compliance period for smaller reporting companies.

In addition, while the proposed disclosures are important, the Commission should also consider the cumulative effects of the burdens placed on public companies when imposing new requirements. Specifically, the Commission should balance the information necessary to ensure investors are kept informed against any burdens placed on public companies based on their size. Without a proper balance, additional burdens may have the unintended impact of making public capital markets a less attractive alternative for companies that consider offering their securities to the public.

Delayed Reporting Should be Permitted Where An Investigation is Ongoing

The Proposal does not provide for a reporting delay for ongoing investigations. If a potential breach was determined to be material, a public company would have concomitant obligations to communicate with customers, comply with statutory and/or regulatory obligations, and communicate with law enforcement within potentially the same four day time period to disclose a cybersecurity incident within the Form 8-K. The Proposal does not provide for a reporting delay for ongoing investigations, even when requested by law enforcement and otherwise permitted under state law and other federal laws. Disclosures of material incidents may serve to hamper an investigation where the scope of the intrusion may yet be unknown, which may strain collaboration with law enforcement. Worse, the obligation to disclose may reveal additional information to an unauthorized intruder who may still have access to the

[3] See proposed Item 106(b).

[4] See proposed Item 106(a).

company's information systems at the time the disclosure is made and potentially further harm the company.[5] The Commission should strongly consider the conflicts raised by disclosure where an investigation is ongoing.

10-K Disclosures Should be Streamlined

Requiring public companies to disclose policies and procedures for identifying and managing cybersecurity risks and governance, including board oversight, as well as management's role and expertise in assessing and managing cybersecurity risks and implementing policies, procedures, and strategies within the Form 10-K would unnecessarily complicate the 10-K filing with information not specifically focused on business operations and financial performance. In 2020, the Commission adopted several amendments designed to modernize and simplify disclosure requirements pursuant to Regulation S-K that apply to periodic reports, proxy statements and certain other public filings.[6] These amendments have streamlined certain disclosure requirements, while also eliminating outdated or duplicative disclosures for reporting companies under Regulation S-K and impacted other forms, among them the Form 10-K. The proposed cybersecurity disclosures[7] could be viewed as counteracting the Commission's goal in 2020 to simplify and streamline disclosure requirements.

If the Commission determines to require the 10-K disclosures, Nasdaq suggests offering public companies a choice to disclose cybersecurity policies and procedures, governance, and management's role and relevant expertise within either the Form 10-K or the proxy statement.

* * *

Nasdaq appreciates the opportunity to respond to the Commission's Proposal and applauds the Commission's actions to enhance and standardize disclosures regarding

---

5 New Item 1.05 would require disclosure of the following information about a material cybersecurity incident, to the extent the information is known at the time of the Form 8-K filing: (1) when the incident was discovered and whether it is ongoing; (2) a brief description of the nature and scope of the incident; (3) whether any data was stolen, altered, accessed, or used for any other unauthorized purpose; (4) the effect of the incident on the registrant's operations; and (5) whether the registrant has remediated or is currently remediating the incident. See Proposal at 16595.

6 See Securities Exchange Act Release No. 89670 (August 26, 2020), 85 FR 63726 (October 8, 2020) (Modernization of Regulation S-K Items 101, 103, and 105).

7 With this Proposal, public companies would be required to include, as part of their Form 10-K, disclosure of: (1) policies and procedures, if any, for identifying and managing cybersecurity risks; (2) a cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks; and (3) management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies. See proposed Item 106(b), (c)(1) and (c)(2) of Regulation S-K.

cybersecurity risk management, strategy, governance, and cybersecurity incidents for public companies. While Nasdaq supports the Proposal's goals to enhance and standardize disclosures regarding cybersecurity, it requests the Commission consider the concerns raised by our listed companies and modify the Proposal to address these concerns.

Thank you for your consideration of our comments. Please feel free to contact me with any questions.

Sincerely yours,

John A. Zecca