May 9, 2022

Via email
rule-comments@sec.gov

Vanessa A. Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-0609

Re: Comments on Proposed Cybersecurity Disclosure Rule - File Number S7-09-22

Dear Ms. Countryman:

LTSE Services, Inc. offers its support for the proposed rule regarding additional disclosure by public companies (and related safe harbors) related to cybersecurity risks entitled "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."[1] We also provide some suggested alternatives for the Securities and Exchange Commission (SEC) to consider in formulating the final rule related to cybersecurity disclosure.

LTSE Services, Inc. is a data and analytics driven capital markets platform specifically designed for public companies and private companies planning to enter the public markets. We strive to help create a more sustainable world by ensuring that public companies that join the LTSE ecosystem have a sustainable business model and are focused on long-term value creation for all of their respective stakeholders.

In this regard, our affiliate, the Long-Term Stock Exchange, Inc., introduced a principles-based approach to addressing sustainability-related issues to differentiate a company's long-term strategy. Underlying this principles-based approach is an understanding that companies consider material environmental, social and governance (ESG) issues, including those related to cybersecurity, that specifically pertain to their businesses and all their respective stakeholders. In doing so, companies are able to identify specific risks and opportunities, and in

[1] *See* 87 F.R. 16590 (2022)

turn, enhance their operating model in order to address these risks and develop a sustainable long-term business strategy. This approach also enables companies to adopt a holistic view and to make fully-informed, sustainable and long-term decisions related to cybersecurity issues for the benefit of all stakeholders.

The proposed rule would amend the current report on Form 8-K to require current disclosure of material cybersecurity incidents. The proposed requirement is to report cybersecurity incidents within four business days after the registrant determines it has experienced a material cybersecurity incident. The evaluation and determination of whether a cybersecurity incident is material to the registrant is complex and takes time to analyze the data and confer with third parties and experts, including a forensics firm that has reviewed the logs and other data related to the incident. Although the rule provides that "[a] registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident," this language is vague and provides insufficient guidance regarding the timing related to the materiality determination that triggers the commencement of the four day reporting period. This requirement could lead to the company reporting incidents prematurely as the initial determination may result in a determination that the incident is material and when new facts surface, it can result in an alternative determination. Further, utilizing the discovery that a cybersecurity incident has occurred as a triggering event, without regard to whether it is material, would result in the reporting of events that may never rise to the level of materiality and only create confusion for investors and unnecessary work and costs for companies.

While we do not dispute that there is a benefit to providing investors with information regarding cybersecurity incidents that are deemed material in a standardized and uniform format as quickly as practicable following the cyber event, the challenge comes with requiring companies to report within 4 business days of a determination that a material cybersecurity event has occurred as this is a difficult determination in many cases and requires significant diligence from the date the incident is discovered. A cybersecurity incident is a fluid situation and determining materiality can be extremely difficult at any given point in time. Unlike the typical Form 8-K event like a change in auditors, or resignation or appointment of a new director or officer, which is an event that is defined in time and largely determined by the company or a director or officer of the company, the determination of the occurrence of a material cybersecurity event is based on facts and circumstances largely out of the control of the company. Requiring this disclosure on a current basis could result in the disclosure of incidents that are not material out of an abundance of caution or additional disclosure delays as companies struggle with the materiality determination and could potentially compromise the ongoing investigation or systems of the registrant depending on the circumstance.[2] As a result, we suggest that the SEC consider

[2] We note that Regulation SCI, which requires disclosure by certain self-regulatory organizations, of certain types of systems events, including cyber intrusion events, to the SEC and the markets, provides some valuable insights regarding the need for potential flexibility in such cybersecurity disclosures. While Regulation SCI provides for immediate notification to the SEC upon the occurrence of a cyber intrusion event concerning an "SCI system" it also provides for a delay in public dissemination of such information, if such notification would compromise the security of applicable "SCI systems." The current proposal lacks this recognition that entities need flexibility in addressing certain types of cyber breaches. *See* 17 CFR § 242.1002(c)(2) (permitting a delay in dissemination of information regarding a systems intrusion if "unless the SCI entity determines that dissemination of such information would likely compromise

making this disclosure part of the periodic reporting process, rather than a current report requirement, as material cybersecurity events are not conducive to reporting on a current basis for the reasons set out above. We agree that material updates to the cybersecurity event disclosure can also be made in the periodic reports, as needed.

If the reporting of a cybersecurity incident is required quarterly, it will generally avoid the potential conflict with other obligations that arise under applicable state and federal laws, as well as conflicts with the ongoing investigation of the event. Exceptions or delays from reporting information should also be permitted where there is conflict with other applicable law or the disclosure would threaten the ongoing investigation.

Given security concerns that could arise with respect to the public disclosure of cybersecurity incidents, as well as policies and procedures related to the identification and management of cybersecurity threats, the SEC should consider clarifying in the final rule that such disclosure should be furnished to the SEC, rather than filed. We also agree that *companies should be afforded the benefit of the safe harbors provided by* Exchange Act Rules 13a-11 and 15d-11 under Exchange Act, particularly in instances where the information is obtained from third parties and public companies are not reasonably able to verify accuracy and completeness of the information provided. Further, we agree that a company should not be penalized with the loss of S-3 eligibility if it experiences a failure to file the Item 1.05 Form 8-K timely.

In addition, given the frequency of cybersecurity incidents, we believe it would be extremely difficult for public companies to have to aggregate multiple cyber incidents to trigger a materiality threshold for disclosure in a periodic report under Item 106(d)(2) of Regulation S-K. That being said, multiple incidents would likely reflect a deficiency in disclosure controls that is material, and such deficiency could lead to a conclusion that disclosure controls and procedures were not effective for such period and disclosed pursuant to such rules.

Finally, the proposal would amend Item 407 of Regulation S-K to require disclosure of whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise. Generally speaking, we believe that if the board does not have a board member who has such expertise it should be sufficient for the board to utilize a third party expert. As a result, we believe that the proposal should be revised to add disclosure regarding whether the board has a cyber expert or utilizes outside resources to advise it on cybersecurity matters if the board members lack sufficient expertise in the area of cybersecurity.

We would like to commend the SEC for its thoughtful consideration of issues related to cybersecurity disclosure and the careful preparation of these proposed disclosure requirements. We appreciate the difficulty in attempting to define requirements applicable to all public companies with respect to an issue which is company-specific in a significant number of respects.

---

the security of the SCI entity's SCI systems or indirect SCI systems, or an investigation of the systems intrusion, and documents the reasons for such determination.").

We believe that the SEC's proposed rule is a step towards ensuring that investors get a clearer and more consistent picture of these issues so that their interests are better protected. The requirement for consistent disclosure of material cyber incidents and impact on the registrant's business, strategy and outlook, as well as the governance of these issues, will help to ensure that due care and full consideration has been given to these risks. We have highlighted changes we believe are necessary to address some inherent concerns we raised regarding the proposal.

As a result of the foregoing, we generally support adoption of the proposed rule, with the changes noted. We believe these changes will cover gaps in current disclosure requirements and address concerns regarding the disclosure of cybersecurity issues in a standardized format.

Thank you for your consideration.

Sincerely,

Martin Alvarez

Martin Alvarez
Chief Commercial Officer

Shahnawaz Malik

Shahnawaz Malik
Head of ESG Analytics

Jane Storero

Jane Storero
Senior Corporate Governance Counsel