NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.
750 First Street, NE, Suite 1140
Washington, DC 20002
202/737-0900
www.nasaa.org

May 9, 2022

Submitted by SEC Webform (http://www.sec.gov/rules/submitcomments.htm)

Vanessa Countryman
Secretary
U.S. 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:

On behalf of the North American Securities Administrators Association, Inc. ("NASAA"),[1] I am writing in response to U.S. Securities and Exchange Commission ("SEC" or the "Commission") Release No. 33-11038, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (the "Proposal").[2] NASAA generally supports the Proposal and encourages its adoption, with certain changes outlined below.

Cybersecurity threats pose considerable risks to public companies, investors, and the U.S. markets as a whole. These risks will only increase in significance as more and more companies venture into fully digital spaces, such as the metaverse.[3] For example, J.P. Morgan Chase & Co. recently opened its "Onyx Lounge," in the Decentraland metaverse, at which visitors to the virtual reality space can walk around and watch exclusive presentations on financial topics through their avatars.[4] As more companies enter these virtual arenas, they will encounter new cybersecurity risks. Phishing in the metaverse "won't be a fake e-mail from your bank . . . . It could be an avatar

[1] Organized in 1919, NASAA is the oldest international organization devoted to investor protection. NASAA's membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico, and the U.S. Virgin Islands. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

[2] The Proposal is available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[3] PwC US, Featured Insights, *Demystifying the metaverse*, https://www.pwc.com/us/en/tech-effect/emerging-tech/demystifying-the-metaverse.html (last visited May 9, 2022) (explaining that the metaverse "is an evolution, not a revolution" and "may profoundly change how businesses and consumers interact," but that the "[r]isks are real too").

[4] *See* Czarina Grace, *JPMorgan Opens a Virtual Lounge in the Metaverse: A $1 Trillion Market Opportunity*, iTech Post (Feb. 16, 2022, 7:02 AM), https://www.itechpost.com/articles/109166/20220216/jpmorgan-jpmorgan-metaverse-decentraland-metajuku-onyx-lounge-jpmorgan-decentraland-how-to-visit-onyx-lounge.htm.

of a teller in a virtual bank lobby asking for your information. It could be an impersonation of your CEO inviting you to a meeting in a malicious virtual conference room."[5] As recognized in the Proposal, cybersecurity risks are both "ongoing and escalating;" in many instances, these risks are existential to the companies in which investors have staked their hard-earned money.[6] Furthermore, large scale cybersecurity incidents can have systemic effects on the broader economy.[7] NASAA is pleased to see that the SEC taking is continuing to take steps to address this issue, as it is critically important to investors and the health of our markets.

The Proposal seeks to enhance and standardize disclosures from public companies about material cybersecurity incidents and companies' cybersecurity risk management. It would do so, broadly, by (1) requiring companies to disclose information about material cybersecurity incidents on Form 8-K within four days of a materiality determination, and to provide quarterly updates to those disclosures as necessary on Forms 10-Q and 10-K (collectively, the "Incident Disclosures"), and (2) requiring companies to disclose information annually about their policies and procedures for identifying and managing cybersecurity risks, including the board's oversight, management's role, and the details of any cybersecurity expertise among the members of the board (collectively, the "Risk Management Disclosures").

I. Incident Disclosures

NASAA generally supports the proposed Incident Disclosure rules. We believe that proposed new Item 1.05 on Form 8-K would provide the markets with clear, comparable, and decision-useful information, and would prove to be a marked improvement from the *status quo*. In particular, we appreciate that Item 1.05 would require disclosure regardless of whether the cybersecurity incident is ongoing.[8] This is an area in which the existing guidance has not led to clear and consistent reporting by public companies.[9] We agree that the information in Item 1.05 would be relevant to investors and other market participants and better enable all to assess the ways in which the incident might impact an investment in the reporting company. We also support the proposed requirements for public companies to include in their quarterly and annual reports any updates regarding previously reported material cybersecurity incidents, as well as information

---

[5] Dina Bass, *Microsoft Security Chief Issues Call to Arms to Protect Metaverse*, Bloomberg (Mar. 28, 2022, 8:45 AM), https://www.bloomberg.com/news/articles/2022-03-28/microsoft-security-chief-urges-focus-on-safety-as-metaverse-is-built (quoting Charlie Bell, Executive Vice President, Security, Compliance, Identity and Management, Microsoft).

[6] *See generally*, Proposal at 5-11.

[7] *See* Proposal at 8.

[8] *See* proposed Item 1.05(a)(1) (requiring disclosure as to "whether [the incident] is ongoing"), Proposal at 127.

[9] *See*, *e.g.*, *In re Alphabet Sec. Litig.*, 1 F.4th 687, 693-98 (summarizing, *inter alia*, the circumstances surrounding the failure to disclose software bugs in the Google+ social network that exposed private user data to third parties), 703 (rejecting the argument that the omission was not materially misleading because the software bugs had already been remediated at the time of the alleged misleading filings) (9th Cir. 2021).

about a series of previously undisclosed individually immaterial cybersecurity incidents that has become material in the aggregate.

We agree that a determination of materiality should be the triggering event for Form 8-K disclosure and that such a determination must be made "as soon as reasonably practicable after discovery of the incident."[10] In our view, these provisions strike the appropriate regulatory balance between the market's need for timely information and a company's need to carefully assess the possible impact of a cybersecurity incident so that it can provide accurate, clear, and decision-useful information. The Proposal acknowledges the possibility that some companies "may delay making such a determination to avoid a disclosure obligation."[11] We believe that the proposed requirement to make the determination "as soon as reasonably practicable" is a reasonable approach to address this concern and provides public companies with the appropriate degree of flexibility to conduct a thorough assessment while ensuring that the markets get timely and relevant information.

Although we generally support the proposed Incident Disclosure requirements, we share the concern expressed by others that the Proposal would not provide for any reporting delay based on an ongoing external investigation related to a cybersecurity incident.[12] Although the Proposal "recognize[s] that a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents," it rejects these concerns without analysis and concludes that "the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay."[13] Respectfully, we believe that this approach would ultimately harm public companies that have already been victimized or targeted, as well as their investors. We, therefore, urge the Commission to revise the Proposal so that the reporting requirements do not inadvertently undermine ongoing law enforcement efforts.

In the aftermath of a cybersecurity incident, law enforcement's need for information is different from that of investors and other market participants. Law enforcement is responsible for investigating potential criminal violations with the goals of identifying, apprehending, and prosecuting the perpetrators.[14] Although law enforcement agencies have many powerful tools at

---

[10] *See* proposed Item 1.05(a) and Instruction 1, Proposal at 127.

[11] Proposal at 22.

[12] *Id.* at 25. *See also* Comm. Hester Peirce, *Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal* (Mar. 9, 2022), https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922 (expressing "concern" that the Proposal is "unduly dismissive of the need to cooperate with, and sometimes defer to, our partners across the federal government and state government," such as where "delaying disclosure about a material cybersecurity incident could increase the chances of recovery of stolen funds or the detection of the wrongdoers in the expert opinion of law enforcement agencies[.]")

[13] Proposal at 25.

[14] *See* U.S. Dep't of Justice, Cybersecurity Unit, *Best Practices for Victim Response and Reporting of Cyber Incidents* ("Best Practices for Victim Response"), 14 (Sept. 2018), https://www.justice.gov/criminal-ccips/file/1096971/download.

their disposal, sometimes it is necessary to control the flow of public information in order to avoid releasing details that might impede an ongoing investigation.[15] We are aware of instances in which law enforcement has requested that the victim delay public disclosure of information about the incident, or withhold certain information, so that law enforcement can identify and locate the perpetrators.[16] A successful law enforcement investigation can provide substantial benefits to public companies, their investors, and the markets by apprehending the bad actors and shutting down their operation or recovering stolen assets or data.[17]

Accordingly, we very strongly encourage the Commission to modify the proposed rule to permit a reporting delay when such a delay is due to a *bona fide* request from any civil or criminal law enforcement agency to delay public disclosure about the cybersecurity incident in question.[18] Such a delay could prove to be the difference between investor protection and investor harm.

II. Risk Management Disclosures

The Risk Management Disclosures generally fall into one of two categories. First, the Proposal would require public companies to disclose certain information about their policies, procedures, and practices, including the board's oversight of cybersecurity risk and management's role in assessing and managing those same risks. Second, the Proposal would require companies to disclose whether any member of the board has cybersecurity expertise and, if so, the name(s) of any such director(s) and such detail as necessary to fully describe the nature of the expertise. NASAA supports the Risk Management Disclosures, and we encourage their adoption, with certain revisions.

We anticipate that some commenters will argue that the Commission is exceeding its authority with respect to public companies and improperly seeking to regulate companies' conduct and operations. We disagree and support the Commission's efforts to ensure that publicly traded companies provide investors with information about the actions they are taking to address cybersecurity risks. The information that would be required to be disclosed under the Proposal is important to investors and other market participants, especially as our economy and market participants become increasingly reliant on technology to engage with employees and customers. It is vital to the health of our markets that public companies take steps to protect themselves by ensuring that leadership understand the risks and by putting in place the necessary policies, procedures, and action plans to protect against cyberattacks and minimize harm once it has

---

[15] *See id.* at 19 (encouraging victims to contact law enforcement, noting that federal law enforcement agencies "will generally coordinate public statements concerning the incident with victim companies to ensure that harmful or sensitive information is not needlessly disclosed[,]" and encouraging "[v]ictim companies [to] consider sharing press releases regarding a cyber incident with investigators before issuing them to avoid releasing information that might impede the ongoing investigation").

[16] NASAA would never advise a regulated entity to disregard a legitimate request from law enforcement.

[17] *See*, *e.g.*, Best Practices for Victim Response at 18-21.

[18] In our view, this would include, but not be limited to, circumstances in which the Attorney General determines that the delay is in the interest of national security. *See* Proposal at 30 (Item 7).

occurred.[19] Investors should have access to this valuable information. Some companies may feel the need to change or update their cybersecurity risk management practices as a result of the required disclosures but, to the extent that this is the case, the motivation for such changes will come from market pressures, not from the SEC. As such, we believe that the proposed disclosure requirements are an appropriate exercise of the Commission's authority regarding public companies.

The Proposal asks whether there are additional aspects of a company's cybersecurity policies and procedures or governance that should be required to be disclosed, as well as whether companies should be required to explicitly state that they have not established any such policies and procedures if that is the case.[20] If a company has not established any cybersecurity policies and procedures, the rule should require that the company state that explicitly. Investors should not be left to intuit the meaning of a company's silence in its disclosures. However, the company should also be required to provide an explanation for why it has not done so. This information would allow investors to fully assess the significance of the company's lack of policies and procedures and make informed investment decisions. This approach would be consistent with the Commission's recent rule proposal regarding Rule 10b5-1 and insider trading.[21] In that proposal, the Commission proposed new Item 408 to Regulation S-K, which would require a public company to "disclose whether [it] has adopted insider trading policies and procedures [and] [i]f the registrant has not adopted such policies and procedures explain why it has not done so."[22] The Commission should impose the same requirement for the Risk Management Disclosures.

The Proposal asks whether the final rule should exempt certain categories of public company registrants from either category of the Risk Management Disclosures, such as smaller reporting companies, emerging growth companies, or foreign private issuers.[23] We would oppose such a change for the reasons already stated in the Proposal:

> [E]vidence suggests that smaller companies may have an equal or greater risk than larger companies of being attacked, making the proposed disclosures particularly important for their investors. The financial impact from an attack could also be more detrimental for smaller companies than for larger ones. To the extent that one indirect effect of the proposed disclosure may be that companies take additional steps to address potential vulnerabilities or enhance their cybersecurity risk management, strategy, and governance, any resulting reduction in vulnerability may be particularly beneficial for smaller companies and their investors.[24]

---

19 *See generally* Best Practices for Victim Response at 1-12.

20 Proposal at 42 (Item 17), 43 (Item 21).

21 *See* Proposed Rule, *Rule 10b5-1 and Insider Trading*, SEC Release No. 33-11013 (Jan. 13, 2022), *available at* https://www.sec.gov/rules/proposed/2022/33-11013.pdf.

22 Proposed Item 408(b)(1), SEC Release No. 33-11013 at 139.

23 Proposal at 43 (Item 23), 47 (Item 35).

24 *Id.* at 86.

These companies should not be exempted from the requirements in the Proposal.

III. Conclusion

NASAA supports the Proposal and encourages its adoption, with certain revisions as explained above. Thank you for considering these views. NASAA looks forward to continuing to work with the Commission in the shared mission to protect investors. Should you have questions, please contact either the undersigned or NASAA's General Counsel, Vince Martinez, at (202) 737-0900.

Sincerely,

Melanie Senter Lubin
NASAA President and
Maryland Securities Commissioner