May 9, 2022

VIA ELECTRONIC SUBMISSION

Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549-1090

Re: Four Business Day Cybersecurity Incident Reporting Requirement under the Proposed Amendment adding Item 1.05 to Form 8-K pursuant to the Securities Exchange Act of 1934 (SEC Release No. 33-11038; IC-34529 File No. S7-09-22; 87 FR 16590 (March 9, 2022))

Dear Ms. Countryman:

The American Investment Council (the "AIC") appreciates the opportunity to submit this letter to the Securities and Exchange Commission (the "SEC") on the proposal to amend Form 8-K to add Item 1.05 (the "Proposed Item") pursuant to the Securities Exchange Act of 1934 (the "Exchange Act").[1]

The AIC is an advocacy, communications, and research organization established to advance access to capital, job creation, retirement security, innovation, and economic growth by promoting responsible long-term investment. In this effort, the AIC develops, analyzes, and distributes information about the private equity and private credit industries and their contributions to the U.S. and global economy. Established in 2007, and formerly known as the Private Equity Growth Capital Council, the AIC is based in Washington, D.C. The AIC's members are the world's leading private equity and private credit firms, united by their commitment to growing and strengthening the businesses in which they invest.[2]

The AIC has supported and continues to support transparency as it relates to cybersecurity risks in the public markets. Because the AIC membership includes registered investment advisers ("RIAs") that invest in the public markets, as well as RIAs with publicly traded parent entities,

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC Release No. 33-11038; IC-34529 File No. S7-09-22; 87 FR 16590 (March 9, 2022) (the "Proposing Release").

[2] For further information about the AIC and its members, please visit our website at http://www.investmentcouncil.org.

the AIC appreciates the opportunity to provide comments on potential challenges that the implementation of the Proposed Item would have on issuers.

This letter contains three sections. The first section identifies the provisions of the Proposed Item that are the subject of this comment letter. The second section highlights the concerns we have in connection with those provisions. The third section proposes alternative solutions and makes recommendations that would further the SEC's goals, while alleviating some of the concerns expressed in the second section.

I. The Proposed Item's Applicability to Issuers

The Proposed Item includes an amendment to Form 8-K that would require issuers to disclose a "material cybersecurity incident" in a Form 8-K filing.[3] Proposed Item 106(a) defines a "cybersecurity incident" as "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."[4]

Issuers would need to file an Item 1.05 Form 8-K within four business days after a determination that the cybersecurity incident was "material" and must make such materiality determinations "as soon as reasonably practicable after discovery of the incident."[5] The disclosure would need to include several details about the incident "to the extent known" by the issuer, including (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 issuer's operations; and (5) whether the issuer has remediated or is currently remediating the incident.[6] An ongoing internal or external investigation would not justify a reporting delay.[7]

II. Why the Proposed Item Is Not Optimal for Meeting the SEC's Objectives

The stated purpose of the Proposed Item is to address a "growing concern that material cybersecurity incidents are underreported and that existing reporting may not be sufficiently timely."[8] The Proposed Item is designed to "provide timely and relevant disclosure to investors and other market participants (such as financial analysts, investment advisers, and portfolio managers) and enable them to assess the possible effects of a material cybersecurity incident on

[3] Proposing Release at 16595-96.

[4] *Id.* at 16601.

[5] *Id.* at 16596.

[6] *Id.* at 16624.

[7] *Id.* at 16596.

[8] *Id.* at 16595.

the registrant, including any long-term and short-term financial effects or operational effects."[9] However, as drafted, the Proposed Item could actually undermine the SEC's mission of protecting investors because it would likely lead to a deluge of vague and inaccurate disclosures to the market, leading to investor confusion as to the likely financial or operational effects of cybersecurity incidents.

In many cybersecurity incidents, very little information is known with any degree of certainty within the first four days, and what is known often turns out to be incorrect or incomplete. For example, suppose a public company first discovers unauthorized activity in its network on a Monday morning. The Company quickly assesses that it was the victim of a ransomware attack, and its defenses appear to have limited the damage to a small number of machines that are not material to its overall operations. The attacker nonetheless claims to have taken a significant amount of data, demands a payment of $1 million, and threatens to release the alleged stolen data if the payment is not made. By Friday morning, in spite of a full-scale investigation that commenced immediately, the Company still cannot confirm that the attacker no longer has any access to its network; the Company can neither confirm nor refute the assertion that data has been stolen; and the attacker has not identified the nature of the data that it allegedly stole. This level of uncertainty is very common in the early days of a cybersecurity incident.

If the Proposed Item were in effect, the Company would have to assess whether this event is a material cybersecurity incident that requires Form 8-K disclosure. The Company would start by confirming that it was an unauthorized occurrence on its information systems that "jeopardizes the confidentiality, integrity, or availability of the Company's information systems" and information residing therein. The Company would then look at the following examples of cybersecurity incidents listed in the Proposed Item that may trigger a Form 8-K disclosure requirement, and conclude that each of them could apply because the company cannot rule out the possibility that the incident is material:

- An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or procedures;
- An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems;
- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

[9] *Id.*

Accordingly, the Company may well conclude that it should make a disclosure, rather than wait for all the relevant facts to become settled, which could take weeks. The Company would understandably be concerned that waiting would create significant risk of a perceived violation of the four-business-day notification deadline if subsequent investigation confirms the materiality of the incident.

The Company would then go through the list of items that must be included in the disclosure "to the extent known," and struggle with each of them because what is known is still very preliminary and could change. For example, as to whether the incident was ongoing, the Company could only say that it might be. As to whether data was stolen, the Company could only say that the attacker has alleged that it has stolen data, and the Company has been unable to confirm that or rule it out, and it does not know whether the stolen data, if any, is sensitive or material. This kind of vague disclosure will confuse investors and could result in an unwarranted plunge in the stock price. If new favorable information about the incident is uncovered over the weekend, the Company would likely feel the need to provide an updated Form 8-K on Monday, which could cause the stock to recover the lost value.

The Proposed Item incentivizes issuers to file "placeholder" disclosures that contain information that is vague or likely to change, in order to avoid any doubt that they have met the four-business-day notification requirement. The resulting flood of ambiguous and equivocal disclosures (which will include notifications for cybersecurity incidents that ultimately turn out not to be material) will undermine the SEC's investor protection mission because investors will not be able to identify the information that actually matters to their investments. Indeed, given the likely volume of 8-Ks that will be of limited value, investors may become numb to these disclosures – which would undercut the SEC's stated purpose of equipping investors and market participants with information to "assess the possible effects of a material cybersecurity incident" on an issuer.

Moreover, premature disclosure of cybersecurity incidents will trigger inquires from customers, counterparties, investors, auditors, the media and regulators. Responding to these inquiries consumes an enormous amount of resources and therefore impedes issuers' efforts to investigate and remediate what may ultimately turn out to be immaterial incidents. Indeed, issuers will likely want to notify many of these stakeholders before filing the Form 8-K, to avoid them learning about the incident indirectly. As such, the early days of incidents will be consumed with drafting notifications to multiple constituencies, and then constantly redrafting them as new information becomes available, diverting precious resources away from responding to and remediating the incident itself.

To reduce these risks, we recommend that the Commission:

- Provide a clarification that by using the words "determined by the registrant to be material" and "information known to the registrant," the SEC intends that a determination of materiality that triggers notification in the Proposed Item should be based on information that is known with a high degree of confidence and is unlikely to change.
- Expand the notification deadline to five business days to ensure that issuers have at least a calendar week to file a Form 8-K, which will provide additional time for facts to be developed that are unlikely to change.

- Provide examples of a "material cybersecurity incident" to limit the confusion that may cause companies to feel obligated to disclose events that could become material, but are not actually material.

III. Proposed Alternatives and Recommendations

Item 1.05 Clarification

The SEC should clarify that the Proposed Item only requires issuers to disclose information that is known with a high degree of confidence and is unlikely to change. Item 1.05 states that if an issuer experiences a cybersecurity incident that it "determine[s] . . . to be material," it must disclose certain information regarding the incident "to the extent known" to the issuer. Without further guidance, it is unclear what degree of confidence the issuer must have regarding whether the information is accurate or likely to change. The public would receive higher quality disclosures that would need fewer updates and revisions with an interpretation in the Final Rule that a determination of materiality that triggers notification should be based on information that is known with a high degree of confidence and is unlikely to change.

Extended Timeline

We believe that an extended reporting timeline to at least five business days (and therefore at least one calendar week) would better serve the SEC's stated goals to provide timely and relevant disclosure to investors and other market participants and enable them to assess the possible effects of a material cybersecurity incident. The additional day would (1) provide issuers with the time they will need to develop relevant facts that are not likely to change, (2) use those facts to conduct a meaningful materiality analysis, and (3) assuming the incident is determined to be material, draft a Form 8-K disclosure that will be relevant and helpful to the market.

Material Incident Examples

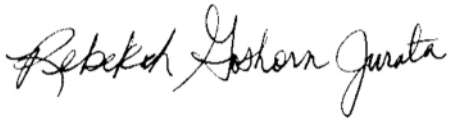
Finally, the SEC should provide concrete examples of cybersecurity incidents that it would consider "material." Although each incident is unique, examples would help issuers make a materiality determination by providing a benchmark for disclosure, which in turn would increase the quality of disclosures and lessen the number of "placeholder" disclosures made containing incomplete information that is of little value to investors. Examples of "material cybersecurity incidents" could include incidents that involve:

- Network operational stoppage for more than [x] hours that has caused harm to a significant portion of the business or a significant number of customers;
- Confirmed ongoing unauthorized access to the company's network for more than [x] days after initial detection; and
- Unauthorized acquisition of sensitive company or customer data that is likely to result in significant business or reputational damage, or harm to a significant number of customers.

*****

The AIC appreciates the opportunity to comment on the Proposed Item and would be pleased to answer any questions that you might have concerning our comments.

Respectfully submitted,



Rebekah Goshorn Jurata
General Counsel
American Investment Council