Debevoise & Plimpton

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
[redacted]

May 9, 2022

Office of the Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-1090

Via email to rule-comments@sec.gov

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

Dear Ms. Countryman:

We appreciate the opportunity to submit this comment letter in response to the request by the U.S. Securities and Exchange Commission (the "Commission") for comments on its release entitled "Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure" (Release Nos. 33-11038; 34-94382; IC-345293; File No. S7-06-22, the "Release"). While we do not seek to comment on every item contained in the Release, we do have concerns and suggestions on specific items, as set forth below.

1. Would investors benefit from current reporting about material cybersecurity incidents on Form 8-K? Does the proposed Form 8-K disclosure requirement appropriately balance the informational needs of investors and the reporting burdens on registrants?

We respectfully submit that the Commission can achieve its goal of providing more timely and fulsome disclosure to investors by augmenting relevant disclosure requirements applicable to Quarterly Reports on Form 10-Q and Annual Reports on Form 10-K (as well as annual reports for Foreign Private Issuers on Form 20-F) and that proposed Item 1.05 of Form 8-K places a potentially undue burden on a registrant experiencing a cybersecurity incident. As such, we do not believe that the Commission should not amend Form 8-K to include proposed Item 1.05. We acknowledge the Commission's concern that disclosure practices regarding cybersecurity incidents vary widely and that investors would benefit from more timely disclosure of such incidents. However, we respectfully submit that augmented cybersecurity incident disclosure requirements would be more appropriately applicable to a registrant's Quarterly Reports on Form 10-Q and Annual Report on Form 10-K, rather than through current reporting. Requiring registrants to include quarterly disclosure regarding cybersecurity incidents that were identified during the period covered by a Form 10-Q or Form 10-K or would afford registrants a greater ability to make public disclosure that is potentially more comprehensive and more usefully contextualized when read in the context of the other required disclosures in such reports (*e.g.*, management's discussion and analysis and the risk factors in the case of a Form 10-K or material updates thereto in the case of a Form 10-Q). This is particularly true in our view given the fact that: (i) cybersecurity is a pervasive threat affecting all registrants; (ii) the investing public is already generally aware of the fact that cyber criminals pose a pervasive threat and that the

potential consequences of cybersecurity incidents is material[1]; and (iii) investors are certainly on notice as to any particular registrant's cybersecurity risks through extant risk factor disclosure practice. To the extent that existing deficiencies in periodic cybersecurity incidents is a motivating factor underlying proposed Item 1.05 of Form 8-K, we suggest that any such inadequacies could be effectively addressed by more comprehensive disclosure requirements applicable to periodic, rather than current, reports filed under the Securities Exchange Act of 1934, as amended (the "Exchange Act").

We also respectfully submit that as a general matter Item 1.05 of Form 8-K imposes potentially undue burdens on registrants that weigh against requiring current disclosure on Form 8-K given the myriad challenges tied to identifying, understanding and managing a cybersecurity incident. In the aftermath of discovery of a cybersecurity incident: (i) a registrant's information gathering may be hampered in the midst of, or by, the incident; (ii) information about the incident available to the registrant may be incomplete or inconclusive; and (iii) a registrant's internal management and compliance resources may be under significant strain. Further, the fact that proposed Item 1.05 is qualitatively different from the other Items requiring disclosure under Form 8-K also argues against adopting proposed Item 1.05 (*i.e.*, the Items required to be disclosed under current Form 8-K generally: (i) relate to events within a registrant's control; (ii) events with respect to which a registrant has some advance warning or awareness; and/or (iii) events that are influenced by a registrant's volitional acts; whereas proposed Item 1.05 would require disclosure of an event that is at its core a matter of registrant reactivity.

4. We are proposing to require registrants to file an Item 1.05 Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. Would the proposed four-business day filing deadline provide sufficient time for registrants to prepare the disclosures that would be required under proposed Item 1.05? Should we modify the timeframe in which a registrant must file a Form 8-K under proposed Item 1.05? If so, what timeframe would be more appropriate for making these disclosures?

See response to Request for Comment 8 below.

7. Should any rule provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?

Should the Commission adopt Item 1.05 of Form 8-K as proposed, we recommend that registrants be permitted to delay reporting of a cybersecurity incident that is the subject of a *bona fide* investigation by law enforcement. As proposed, Item 1.05 does not provide for a reporting delay (beyond the standard four-business-day filing requirement) when there is an ongoing internal or external investigation related to a cybersecurity incident. In the relevant discussion in the Release, the Commission recognizes that "a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents." We respectfully suggest that the Commission should

[1] Various studies and reports cited by the Commission in the Release support this conclusion (*See* the Release at footnote 19).

consider whether appropriate consideration has been given as to the necessity to delay such disclosure in the context of an ongoing investigation (particularly by law enforcement). A delay in reporting may not only facilitate such an investigation, it may be critical to its success. We are concerned that requiring Item 1.05 disclosure to be filed within the standard four-business-day Form 8-K filing requirement without exception will more likely alert cybercriminals to detection of their infiltration, which could enable them to abscond prior to apprehension or before the relevant methods of infiltration and exfiltration used by the criminals have been analyzed and mapped. This would have the effect of depriving the commercial sector and law enforcement agencies alike of the knowledge base necessary to more effectively address ongoing and future cybersecurity incidents. Further, to the extent that a registrant receives an official request from a law enforcement agency or body, the inability to honor such a request would put the registrant in an awkward opposite position with such agency or body and potentially and irrevocably harm the relevant investigation.[2] Finally, we are concerned that the Release includes little discussion or seems to reflect inadequate consideration of the national security implications of current (and potentially premature) disclosure of a cybersecurity incident under proposed Item 1.05 of Form 8-K. A failure to apprehend cybercriminals and fully analyze the relevant methods of infiltration and exfiltration deprives the national security firmament of tools necessary to address constantly evolving cybersecurity threats. In particular, we note that these potential harms to national security from a premature disclosure are at their most severe in the context of a cybersecurity incident at a registrant with government contracts or with a business that is focused on national security matters. We believe that modestly amending the proposed cybersecurity disclosure requirements such that registrants are sufficiently able to manage a cybersecurity incident out of the public eye is of nationally significant import.

As noted above, assuming that Form 8-K is amended to include Item 1.05 as proposed, we recommend that the Commission include an exception from the current reporting requirement under Item 1.05 of Form 8-K when a cybersecurity incident is the subject of a *bona fide* investigation by law enforcement. Any such delayed disclosure should, of course, be required to be made under cover of Form 8-K (or a proximate periodic report if appropriate) as soon as is reasonably practicable. We also believe that an analogous exception should be adopted such that a registrant is not required to make "premature" disclosure of a *bona fide* internal investigation under cover of Forms 10-Q or 10-K ("Periodic Reports"). As a means to ensure that registrants utilize such an exemption appropriately, we suggest that the Commission could require a registrant delaying disclosure of a cybersecurity incident in a Form 8-K or in a Periodic Report to include the following disclosure in the current or periodic report in which the disclosure is ultimately filed: (i) confirmation of the fact that the incident was the subject of an investigation; and (ii) the basis for utilizing the filing delay.

[2] In this regard, we believe that the Commission's suggestion to narrow such an exception to requests by the Attorney General for such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security would materially diminish the utility of such an exception give the potentially short Form 8-K filing deadline. Instead, should the Commission adopt an exception that is narrower than what we have recommended above, we suggest that: (i) senior officials of other offices/agencies/departments of the U.S. government (*e.g.*, Federal Bureau of Investigation ("FBI") be included within the universe of persons who may make such a request and (ii) less senior (but sufficiently credentialed) officials at each such office/agency/department (*e.g.*, an Assistant Attorney General or, in the case of the FBI, an Executive Assistant Director) be authorized to make such a request.

8. We are proposing to include an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Is this instruction sufficient to mitigate the risk of a registrant delaying a materiality determination? Should we consider further guidance regarding the timing of a materiality determination? Should we, for example, suggest examples of timeframes that would (or would not), in most circumstances, be considered prompt?

We respectfully submit that, should proposed Item 1.05 be adopted as is, the ambiguity inherent in Instruction 1 to proposed Item 1.05 will make it difficult for a registrant to determine whether it is compliant with its current reporting obligations under Form 8-K. We are also concerned that providing examples of "timeframes that would (or would not), in most circumstances, be considered prompt" will provide investors with a false sense of certainty as to the completeness of the disclosure in the context of highly variable, fluid and uncertain events. Instead, as noted above, we respectfully suggest that Form 8-K not be amended to include proposed Item 1.05.

To the extent that the Commission adopts Item 1.05 to Form 8-K as proposed, we recommend that the Commission make the following modifications: (i) revise the filing trigger for Item 1.05 Form 8-K such that a disclosure is required following a determination by the registrant that it has experienced a material cybersecurity event; but only to the extent that the information upon which the determination is based has been deemed by the registrant to be (a) verified by the registrant as accurate with a high degree of confidence and (b) unlikely to materially change; and (ii) lengthen the filing requirement by at least one business day within which an Item 1.05 Form 8-K is required to be filed (*i.e.*, the Form would be required to be filed within 5 business days of the registrant's determination). We believe that these two changes would increase certainty in a registrant's disclosure and appropriately balance the Commission's objectives of timely disclosure against the burdens on a registrant in the context of a cybersecurity incident.

13. Should we include Item 1.05 in the Exchange Act Rules 13a-11 and 15d-11 safe harbors from public and private claims under Exchange Act Section 10(b) and Rule 10b-5 for failure to timely file a Form 8-K, as proposed?

See response to Request for Comment 14 below.

14. Should we include Item 1.05, as proposed, in the list of Form 8-K items where failure to timely file a Form 8-K will not result in the loss of a registrant's eligibility to file a registration statement on Form S-3 and Form SF-3?

We believe that the proposed amendments to Form S-3 and F-3 and to the Exchange Act safe harbor provisions noted above are appropriate and warranted. Given the uncertainties inherent in and the burdens related to the production of disclosures relating to cybersecurity incidents (particularly at or shortly following discovery), noted above, we agree with the Commission that: (i) a loss of Form S-3 or F-3 eligibility due to a failure to timely file an Item 1.05 Form 8-K would be unduly harsh; and (ii) inclusion of Item 1.05 in the list of Form 8-K items eligible for the safe harbor is warranted. We also believe that the inclusion of Item 1.05 Form 8-K(s) as per items (i) and (ii) above would further the Commission's goal of facilitating

the provision of "more timely and consistent disclosure about material cybersecurity incidents" across registrants.

18. Are the proposed definitions of the terms "cybersecurity incident," "cybersecurity threat," and "information systems," in Item 106(a) appropriate or should they be revised? Are there other terms used in the proposed amendments that we should define?

We note that the definition of "cybersecurity threat" as proposed means: "any potential occurrence that *may* result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein" (*emphasis added).* We respectfully suggest that the use of a "may" standard establishes an unhelpfully low standard that would require registrants to establish policies and procedures that are potentially overbroad and not appropriately tailored to those threats that are reasonably foreseeable. As such, we recommend that the definition of "cybersecurity threat" be revised by replacing "may" with "could reasonably be expected to".

38. **Should we amend Form 20-F, as proposed to require disclosure regarding cybersecurity risk management and strategy, governance, and incidents? Additionally, should we amend Form 6-K, as proposed, to add "cybersecurity incidents" as a reporting topic? Are there unique considerations with respect to FPIs in these contexts?**

We respectfully suggest to the Commission that the disclosure of a cybersecurity incident by a foreign private issuer presents the same issues and considerations as those noted in our responses above. As such, we believe that it would be appropriate to amend the filing and disclosure requirements set forth in the Release in sync with the amendments we recommend above for domestic issuers.

* * *

We appreciate the opportunity to submit for the Commission's consideration our comments on the Release as set forth herein. We would be pleased to discuss our comments with you or provide any additional information you would find useful. If you have any questions regarding this letter, please do not hesitate to contact Matthew Kaplan at [redacted].

Respectfully submitted,

/s/ Matthew E. Kaplan

By: Matthew E. Kaplan
OBO: Debevoise & Plimpton LLP