MORRISON FOERSTER

250 WEST 55TH STREET
NEW YORK, NY 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

AUSTIN, BEIJING, BERLIN, BOSTON, BRUSSELS, DENVER, HONG KONG, LONDON, LOS ANGELES, NEW YORK, PALO ALTO, SAN DIEGO, SAN FRANCISCO, SHANGHAI, SINGAPORE, TOKYO, WASHINGTON, D.C.

May 9, 2022

Writers' Direct Contacts
+1 (212) 506.7213
MWugmeister@mofo.com

+1 (212) 336.4409
HMarlier@mofo.com

Vanessa A Countryman
Secretary
Securities and Exchange Commission
100 F Street NE, Washington, DC 20549-1090

Re: Comments of the Global Privacy Alliance on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SR-09-22, 87 FR 16590

Dear Secretary Countryman:

The Global Privacy Alliance ("GPA") welcomes the opportunity to comment on the proposed rule regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies (the "Cybersecurity Rule"), issued by the Securities and Exchange Commission (the "Commission") and as published on March 23, 2022.[1]

The GPA is comprised of a cross section of public companies and other global businesses from the automobile, aerospace, communications, computer and computer software, consumer products, electronic commerce, financial services, logistics, pharmaceutical, medical devices, and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy and data security obligations seriously. The views expressed in this letter generally represent the views of the members of the GPA. While all members support the overall approach presented, certain of the individual points raised may not be relevant to, or shared by, all members.

The GPA offers comments on three aspects of the Cybersecurity Rule, which, if implemented in its current form, could hamper law enforcement investigations of serious cybersecurity incidents and result in uninformed, or partially informed, disclosures that may not provide investors with the transparency the proposed rule seeks to achieve. First, the Cybersecurity Rule's proposed disclosure requirements lack a much needed law enforcement exception to the four-business-day disclosure deadline for cybersecurity incidents deemed to be material. Second, the Cybersecurity Rule, as written, provides insufficient guidance to

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590 (Mar. 23, 2022) (to be codified at 17 C.F.R. 229, 232, 239, 240, 249).

public companies as to when immaterial cybersecurity incidents become material in the aggregate, and the time period over which public companies should assess and analyze immaterial incidents for aggregation purposes. Third, the Cybersecurity Rule's proposed requirement that issuers should provide specific information about their cybersecurity risk management and strategy, including a description of their risk assessment program and identification and management of cybersecurity risks and threats, may very well subject public companies to further attacks as bad actors can use these disclosures as a roadmap.

A Final Cybersecurity Disclosure Rule Should Include a Law Enforcement Exception

An important way that public companies learn that they have been the victim of a cybersecurity attack is through law enforcement notification. These notifications often include information that law enforcement agencies need to keep confidential in order to apprehend a bad actor. Thus, a law enforcement exception is essential to both holding cyber criminals accountable and ensuring that public companies are notified that they have been attacked. Indeed, as the SEC's 2018 guidance on cybersecurity disclosures noted, "We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident."[2]

The proposed Cybersecurity Rule, however, explicitly declines to provide for this essential disclosure exception, with limited explanation as to why the Commission is reversing course from prior guidance. The Cybersecurity Rule would amend Form 8-K to add a new Item 1.05 that would require an issuer to disclose known information about a material cybersecurity incident within four business days of its materiality determination.[3] It would not provide for any disclosure delay due to ongoing law enforcement investigations, although the Cybersecurity Rule 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."[4] Indeed, the Cybersecurity Rule brushes aside law enforcement considerations, and state and federal laws that explicitly provide for a law enforcement exception, to conclude that disclosures to investors should trump apprehension of cybercriminals.

---

[2] Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166, 8,169 (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[3] If the date of the materiality determination becomes the trigger for the four-business-day reporting deadline, the Cybersecurity Rule states that the Commission "expect[s] registrants to be diligent in making a materiality determination in as prompt a manner as feasible." Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. at 16,596.

[4] *Id.*

Our members work closely with law enforcement agencies on cybersecurity matters and believe that the lack of a specific law enforcement exception to disclosure will harm the broader public, including investors. Companies often learn from law enforcement that cybercriminals have attacked them. This information can be based on sensitive information obtained from confidential sources and methods that would be compromised if prematurely disclosed. Once public companies receive information about a cyberattack from law enforcement, frequently they cooperate with law enforcement on operations that will enable law enforcement to disrupt malicious cyber actors or prevent future attacks—operations that may take longer than four business days to execute. If law enforcement agencies know that public companies may have an obligation to disclose information shared with them within a matter of days, they may be less willing to make such victim notifications and there may be fewer opportunities to disrupt or prevent criminal activity, thereby putting companies and investors at greater risk.

The proposed Cybersecurity Rule's lack of a law enforcement exception is also inconsistent with the laws of all 50 states, Washington D.C., and Guam concerning cybersecurity breach notification. An important feature of the state breach laws is victim notification. These myriad laws generally provide that law enforcement agencies must notify victims of a cyber-breach, but law enforcement can request that a company keep the information confidential from customers and other potential victims. In our experience, such provisions have been used infrequently and have not been abused by law enforcement agencies.

Yet there is a disharmony between the proposed Cybersecurity Rule, which declines to recognize a law enforcement exception, and these state breach notification laws, which appreciate and incorporate this necessary exception. While the former requires that public notice of the incident be given within a short and strict timeframe after the materiality determination, the latter have all agreed that apprehension of cybercriminals justifies delayed disclosure in certain, limited circumstances. These divergent approaches could result in uneven information flows, with the potential for news of an incident to reach unaffected third-parties before individualized notice is given to customers and others who are directly harmed.[5]

The Commission's notice of proposed rulemaking asks for comment on whether the rule should "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?"[6] The answer, in our view, is "yes"—we believe that a delay of

[5] Indeed, if adopted, the proposed rule's disclosure obligations may also conflict with soon-to-be adopted *confidential* reporting obligations to Cybersecurity and Infrastructure Security Agency (or CISA), which will apply to critical infrastructure providers. Consolidated Appropriations Act 2022, Pub. L. No. 117-103, § 2242, 136 Stat. 49 (2022) (Cyber Incident Reporting for Critical Infrastructure Act).

[6] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. at 16,598.

disclosure in such circumstances would be essential and that national security concerns should trump timely notification to investors. But we also believe that the question frames the issue too narrowly in two respects.

First, the exclusion for law enforcement should not be limited solely to the national security context. There are many cybersecurity incidents that present significant public safety concerns, but not necessarily national security concerns, such as incidents involving sophisticated criminal organizations. The delay provision, therefore, should apply to situations affecting both national security, public safety, and other important interests.

Second, the Attorney General should not be the only official who can make a determination of the impact to national security, public safety or other concerns. Numerous law enforcement agencies provide notices of cybersecurity incidents, and do so notwithstanding ongoing sensitive investigations. Such agencies include the U.S. Secret Service, U.S. Customs and Border Patrol, the U.S. Department of Commerce's Bureau of Industry and Security, the Treasury Department's Financial Crimes Enforcement Network, and numerous law enforcement agencies within the Department of Defense and Intelligence Community. Rather than allowing such determinations to be made solely by the Attorney General, the rule should allow any head of a law enforcement agency to make such a determination.

The Proposed Rule Lacks Sufficient Guidance on How, and When, to Make Aggregated Materiality Determinations for Individually Immaterial Cybersecurity Incidents

The proposed requirement that public companies disclose "when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate"[7] lacks much needed guidance and, as a practical matter, may be a solution in search of a problem. The proposed rule would include a Proposed Item 106(d)(2) of Regulation S-K, requiring public companies to analyze related cybersecurity incidents for materiality, both individually and in the aggregate.[8] Other than providing a nonspecific example that "a number of smaller but continuous cyber-attacks related in time and form against the same company"[9] could be material in the aggregate, the proposed rule lacks guidance on (1) when immaterial incidents can become material, quantitatively or qualitatively, in the aggregate and (2) the time period over which public companies must aggregate immaterial cybersecurity incidents.

---

[7] *Id.* at 16,599.
[8] *Id.*
[9] *Id.*

First, public companies need guidance on when immaterial incidents can become material.[10] Many public companies face a barrage of disparate, immaterial cybersecurity incidents in any given quarter, ranging from things like laptop or smartphone theft to unsuccessful phishing scams.[11] As a practical matter, it is hard to envision a scenario where these unrelated, immaterial incidents have such an aggregate impact on a company's operations and financial statements that they amount to a material incident. To the extent that the Commission has some basis for proposing this disclosure requirement, more guidance is essential. For example, what makes a cybersecurity incident "related" to other incidents? Does the proposed requirement mean that public companies must track each and every immaterial cybersecurity incident to plan for the very unlikely event that they may be material in the aggregate? In practice, this proposed disclosure requirement will create inefficiencies and extra work for IT and legal departments alike with very little likelihood that investors will receive any additional information of benefit to their investing decisions.

Second, the proposed requirement that companies disclose immaterial incidents that become material in the aggregate is lacking a much needed time period over which companies must aggregate individual and immaterial incidents. Must companies track each and every immaterial cybersecurity incident—which could include every attempted phishing scam, malware installation, or hardware theft—into perpetuity? Or, conversely, must public company legal departments conduct a quarterly review of all immaterial incidents, effectively wiping the slate clean each quarter? The onus of the first approach (i.e. perpetual tracking of immaterial incidents) on large public companies is obviously immense. But even a quarterly review of each and every immaterial cybersecurity incident places a huge burden on IT and legal groups. Many public companies are the victims of near daily, unsuccessful and immaterial cybersecurity attacks. A quarterly review would require logging, categorization, review, and discussion of minor incidents, taking valuable resources away from managing the day-to-day business operations that are critical to investor satisfaction.

Public Companies Should Not be Compelled to Provide Cyber Criminals an Attack Roadmap Via Disclosure of Their Cybersecurity Policies and Procedures

In 2018, the Commission stressed, appropriately, the real need for public companies to adopt and implement policies and procedures that are tailored to the unique risks that each company faces.[12] Our members take this guidance very seriously. In 2018, the Commission

---

[10] Indeed, even the examples of *material* cybersecurity incidents provided in the proposed rule itself may not meet the materiality threshold under the SEC's 2018 guidance.

[11] These numerous and frequently occurring examples do not meet the current materiality threshold, but, without more specific guidance on the timing and manner of disclosure required, these events could lead to a massive increase in notifications to investors about breaches, diluting the effect of communications generally and detracting focus from breaches that are truly material.

[12] Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8,169.

also recognized that a requirement that public companies make detailed disclosures about their cybersecurity risk management could provide "a 'roadmap' for those who seek to penetrate a company's security protections."[13] The Commission appears to have shifted course without guidance or clarification. The proposed Cybersecurity Rule's mandate that companies disclose policies and procedures for cybersecurity risk management will give cybercriminals exactly the type of roadmap that the Commission expressed concern about just four years ago.

If enacted, the proposed rule would add proposed Item 106(b) to Regulation S-K, requiring issuers to describe in Form 10-K their "policies and procedures, if any, for the identification and management of risks from cybersecurity threats."[14] These include identification of policies and procedures to identify and manage cyber-related risks and threats, including operational risk, intellectual property theft, fraud, extortion, harm to employees or customers, legal violations and risks, and reputational risks.[15] Proposed Items 106(b)(1), (3), (4), (6), and (7) are of particular concern to our members: collectively, these proposed items provide direction to cybercriminals of how to spot vulnerabilities and what to disable if they gain access to an issuer's IT environment.[16] For example, requiring public companies to disclose whether and how cybersecurity considerations affect the selection and oversight of third-parties, including the contractual and other mechanisms the company uses to mitigate risk, could expose companies to malicious actors focused on identifying patterns of selection and potentially put companies at a competitive disadvantage if detailed information is publicly available. Requiring public companies to provide more than confirmation of the existence of policies helps neither companies nor investors and may subject public companies to additional litigation risks. Similarly, proposed Item 106(d)(1)'s requirement that public

---

[13] *Id*.
[14] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. at 16,593.
[15] *Id.* at 16,600.
[16] Disclosures made under proposed Item 106(b) would discuss whether:

"(1) The registrant has a cybersecurity risk assessment program, and if so, provide a description of such program; . . .
(3) The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider, including, but not limited to, those providers that have access to the registrant's customer and employee data [and] . . . the registrant shall describe these policies and procedures, including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers;
(4) The registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents, and if so, provide a description of the types of activities undertaken; . . .
(6) Previous cybersecurity incidents informed changes in the registrant's governance, policies and procedures, or technologies; [and]
(7) Cybersecurity-related risks and previous cybersecurity-related incidents have affected or are reasonably likely to affect the registrant's strategy, business model, results of operations, or financial condition and if so, how[.]" *Id.* at 16,622.

companies disclose any changes in a company's policies and procedures as a result of a material cybersecurity incident serves to highlight potential vulnerabilities for cybercriminals.

Our members are concerned that the proposed Item 106(b) disclosures will undermine their cybersecurity defense efforts and make them more vulnerable to serious cybersecurity attacks. This will harm not only public companies, but their investors and capital markets as well. The federal securities laws disclosure regime is grounded in materiality: investors are best protected when they receive material information about public companies. The level of specificity contemplated by the proposed changes to Item 106, however, will not increase the flow of material information to investors (which is already happening under the current framework) but will make the very companies they invest in more susceptible to cyberattacks.

Conclusion

Certain aspects of the proposed Cybersecurity Rule—namely, the lack of a law enforcement exception to the four-business-day disclosure requirement, the requirement to disclose certain immaterial incidents, and the mandate to disclose cybersecurity risk management policies and procedures—are an unnecessary and potentially harmful departure from the current materiality-based disclosure regime. The lack of a law enforcement exception will chill law enforcement notification of companies that have been attacked, leaving companies and their customers unaware that they have been victimized, and will prevent companies from cooperating with law enforcement to apprehend cybercriminals. The requirement that companies disclose immaterial cybersecurity incidents that, in the aggregate, become material is unworkable without further guidance as to the types of incidents the Commission is contemplating and a time period to prevent perpetual logging and re-reviewing of immaterial incidents. And, finally, the requirement that companies disclose specifics about their cybersecurity risk management, including activities they undertake to prevent and detect attacks, will only increase the harm that companies and investors face by providing cybercriminals with a roadmap of companies' IT environments and vulnerabilities. By contrast, the existing disclosure regime, which is grounded in materiality, protects both investors and the public companies in which they invest.

Sincerely,

Miriam Wugmeister

Miriam H. Wugmeister

Haimavathi V. Marlier