John W. White
+1-212-474-1732
jwhite@cravath.com

David J. Kappos
+1-212-474-1168
dkappos@cravath.com

Timothy G. Cameron
+1-212-474-1120
tcameron@cravath.com

John D. Buretta
+1-212-474-1260
jburetta@cravath.com

Evan Norris
+1-212-474-1524
enorris@cravath.com

Michael L. Arnold
+1-212-474-1664
marnold@cravath.com

Kimberley S. Drexler
+1-212-474-1434
kdrexler@cravath.com

SEC Proposes Rules To Enhance and Standardize Cybersecurity-Related Disclosure for Public Companies

March 17, 2022

On March 9, 2022, the Securities and Exchange Commission (the "SEC" or the "Commission") held an Open Meeting at which the commissioners voted to propose for public comment new rules for public companies related to disclosures of cybersecurity incidents, risk management, strategy and governance (the "Proposed Rules"). The Proposed Rules include amendments to Form 8-K to require current disclosure by public companies of material cybersecurity incidents; amendments to Regulation S-K to require public companies to provide updated cybersecurity-related disclosure in periodic reports on Forms 10-Q and 10-K as well as proxy statements; corresponding amendments to annual reports on Form 20-F to require the same periodic disclosure for foreign private issuers ("FPIs") as proposed for domestic public companies; and new requirements that companies provide the proposed disclosures in Inline XBRL. If adopted as proposed, these rules will create the first cybersecurity-specific disclosure obligations for public companies, and we expect they will lead to operational and governance changes for many companies.

Under the Proposed Rules, a public company would have four business days to report, pursuant to a new Item 1.05 of Form 8-K, any cybersecurity incident that the company has determined is material. Public companies would also be required to include in their periodic reports on Forms 10-Q and 10-K updates regarding previously reported cybersecurity incidents. The Proposed Rules would also add new disclosure requirements for public companies' annual reports on Form 10-K regarding their policies and procedures regarding cybersecurity risks, as well as about their board's oversight of such risks and management's role in assessing and managing cybersecurity risks and implementing cybersecurity policies, procedures and strategies. Finally, public companies would be required to include in their Form 10-K and proxy statements information about which, if any, members of their board of directors has expertise in cybersecurity and the nature of that expertise. The Proposed Rules would expand and codify guidance from both the SEC and the agency's staff (the "Staff") that has previously been released, extensively widening the disclosure requirements for public companies regarding cybersecurity matters.

Comments on the Proposed Rules may be submitted until the later of May 9, 2022 (*i.e.*, 60 days from publication on the SEC's website at https://www.sec.gov/rules/proposed/2022/33-11038.pdf) and 30 days from publication in the Federal Register.

PRIOR SEC INTERPRETIVE GUIDANCE AND RULEMAKING REGARDING CYBERSECURITY DISCLOSURE

The Proposed Rules follow a series of issuances of interpretive guidance regarding disclosure related to cybersecurity risks and incidents. In 2011, the Staff issued interpretive guidance (the "2011 Staff Guidance") providing the Staff's views regarding cybersecurity-related disclosure in risk factors, management's discussion and analysis of financial condition and results of operations, description of business, disclosure concerning legal proceedings and financial statement disclosures. In 2018, the Commission issued its own interpretive guidance (the "2018 Interpretive Release") that reinforced and expanded upon the 2011 Staff Guidance, particularly noting the importance of companies maintaining robust disclosure controls and procedures to enable them to make accurate and timely disclosure of cybersecurity-related material events and reminding companies and corporate insiders of the application of insider trading prohibitions to such incidents. The 2018 Interpretive Release also provided that the materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of any impact on company operations depends upon (1) the nature, extent and potential magnitude of the risks and incidents and (2) the range of harm that such incidents could cause, including reputation, financial performance, and customer and vendor relationships. Under the Proposed Rules, both the 2011 Staff Guidance and the 2018 Interpretive Release would continue to apply.

Cybersecurity emerged as an early priority of the SEC under Chair Gary Gensler. On June 11, 2021, the SEC included cybersecurity risk governance in its annual regulatory agenda. Chair Gensler also discussed the potential for proposals addressing cyber hygiene and incident reporting in Congressional testimony and a speech in September 2021 and signaled upcoming proposed rules in a speech on January 24, 2022. On January 26, 2022, the SEC proposed rules to enhance investor protections and cybersecurity by expanding Regulation ATS for alternative trading systems ("ATSs") that trade government securities, NMS stock and other securities, extending Regulation Systems Compliance and Integrity to ATSs that trade government securities and amending the SEC rule regarding the definition of an "exchange". On February 9, 2022, the SEC proposed new rules and amendments that would, for the first time, impose cybersecurity compliance and disclosure requirements on investment advisers under the Investment Advisers Act of 1940 and investment companies ("Funds") under the Investment Company Act of 1940. The proposed rules and amendments would require investment advisers and Funds to implement certain policies and procedures that are reasonably designed to address cybersecurity risks, include an annual review to assess the effectiveness of such policies and procedures and, in the case of Funds, include oversight by the Fund's board of directors. The proposed rules and amendments also require investment advisers and Funds to keep cybersecurity-related books and records, report significant cybersecurity incidents within 48 hours, disclose cybersecurity risks and incidents and, in the case of Funds, disclose significant cybersecurity incidents from the last two years. The Proposed Rules continue this trend, with the SEC continuing to sharpen its focus on cybersecurity disclosures and internal controls.

DISCLOSURE OF MATERIAL CYBERSECURITY INCIDENTS IN CURRENT REPORTS

The Proposed Rules would require U.S. domestic public companies to disclose material cybersecurity incidents in a current report on Form 8-K within four business days after the company determines that it has experienced an incident and that the incident is material.[1] The amendment to Form 8-K would add a new Item 1.05 requiring the disclosure of when the incident was discovered, whether it is ongoing, a brief description of the nature and scope of the incident, whether any data was stolen, altered, accessed, or used for any other unauthorized purposes, the effect of the incident on the company's operations and whether the company has remediated or is currently remediating the incident.

Although companies may determine certain significant cybersecurity incidents to be material simply upon discovering the incident, the SEC recognized that in some situations materiality determinations may occur after the date of discovery. Accordingly, the Commission's release for the Proposed Rules expressly states that the Form 8-K trigger will be the date of determination of materiality, not the discovery of the incident. Under Instruction 1 to proposed Item 1.05, the SEC would require that a company "make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident". Without repeating the materiality determination guidance in the 2018 Interpretive Release, the Proposed Rules provide that when a cybersecurity incident occurs, companies would need to carefully assess whether the incident is material in light of the specific

circumstances presented by applying a well-reasoned, objective approach from a reasonable investor's perspective based on the total mix of information.

The SEC provided a non-exclusive list of examples of cybersecurity incidents that could trigger the proposed Item 1.05 disclosure requirement. These include:

- An unauthorized incident that has compromised the confidentiality, integrity or availability of an information asset (data, system or network) or violated the company's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;
- 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 company;
- 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.

Additionally, the SEC specified that an ongoing internal or external investigation would not on its own provide a basis for avoiding disclosure of a material cybersecurity incident. The Proposed Rules would provide that the untimely filing of an Item 1.05 8-K would not result in the loss of Form S-3 eligibility and that disclosure under Item 1.05 would be eligible for a limited safe harbor from liability under Section 10(b) of the Securities Exchange Act of 1934 or Rule 10b-5 thereunder.

The SEC also proposed an amendment to General Instruction B of Form 6-K to include material cybersecurity incidents among the list of items that may trigger a current report on Form 6-K for FPIs. A Form 6-K is required for information an FPI (1) makes or is required to make public under the laws of its jurisdiction of incorporation, (2) files, or is required to file under the rules of any stock exchange or (3) otherwise distributes to its security holders. Form 6-K includes a list of items that may trigger this requirement, such as information about acquisitions or dispositions, material legal proceedings or changes in management or control. The Proposed Rules would add "cybersecurity incidents" to this list.

RECURRING CYBERSECURITY-RELATED DISCLOSURE

The Proposed Rules would require cybersecurity-related disclosures in companies' annual reports on Form 10-K pursuant to proposed Item 106 of Regulation S-K. Observing that most public companies that disclosed a cybersecurity incident in 2021 did not describe their cybersecurity risk oversight and related policies and procedures, the SEC has proposed Item 106(b), which would require disclosure of any policies and procedures by which a company identifies and manages cybersecurity risks and threats, the impact of cybersecurity risks on a company's business strategy and whether cybersecurity risk and previous incidents have affected or are reasonably likely to affect a company's results of operations or financial condition. Proposed Item 106(c) would require disclosure of a company's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of persons in positions or on committees responsible for managing cybersecurity risks, and management's role in implementing the company's cybersecurity policies, procedures, and strategies. Proposed Item 106(d)(1) would require companies to disclose any material changes, additions or updates to information required to be disclosed pursuant to proposed Item 1.05 of Form 8-K. Finally, proposed Item 106(d)(2) would require disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents becomes material in the aggregate. Disclosures pursuant to new Item 106(d) of Regulation S-K would be required in quarterly reports on Form 10-Q as well as in the annual report on Form 10-K.

The SEC also proposed requiring cybersecurity-related disclosure in proxy statements and information statements when action is taken with respect to the election of directors. Proposed Item 407(j) of Regulation S-K would require that if any member of the board of directors of a company has cybersecurity expertise, the company would disclose the name(s) of any such director(s) and describe the nature of the expertise. The Proposed Rules would not define what constitutes "cybersecurity expertise", identifying only a non-exclusive list of criteria, but they would state that a person who is determined to have expertise in cybersecurity would not be deemed an expert for any purpose nor have greater cybersecurity-related duties, obligations or liability than other members of the board. The SEC's language around cybersecurity expertise is reminiscent of the safe harbor the SEC created for audit committee financial experts in 2003—expressly confirming that such a designation does not make the director an expert for purposes of Section 11 of the Securities Act of 1933 and does not result in any other greater liability for a director identified as having such expertise.

Additionally, the Proposed Rules would amend Form 20-F to add Item 16J requiring an FPI to include in its annual report on Form 20-F the same type of disclosure as proposed for domestic public companies in their periodic reports and proxy or information statements.

Under the Proposed Rules, all of the information specified by Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K must be tagged in Inline XBRL, including both block text tagging of narrative disclosures and detail tagging of quantitative amounts disclosed within narrative disclosures.

ANALYSIS

The Proposed Rules represent a significant expansion of the SEC's emphasis on cybersecurity disclosures and related policies and procedures, and if adopted, they may result in a significant amount of effort for companies to build out compliance procedures. For example, we expect one area of comment on the Proposed Rules to be the difficulty of complying with the proposed Item 1.05 requirement for current reporting on Form 8-K within four business days of a company experiencing a material cybersecurity incident. Cybersecurity incidents often require significant investigation to determine the precise facts of what has occurred, and a comprehensive evaluation of the consequences of an incident may not be clear for a significant period of time. The SEC has clearly anticipated potential objections from registrants, however, having stated within the Proposed Rules, "it is critical to investor protection and well-functioning, orderly, and efficient markets that investors promptly receive information regarding material cybersecurity incidents". In his remarks accompanying the proposing release for the Proposed Rules, SEC Chair Gary Gensler also emphasized that disclosure of such events should be timely. Although the necessary and sometimes time-consuming work required to make a materiality determination regarding a cybersecurity incident may delay a company's requirement to disclose an incident, we expect that the instruction to make a materiality determination as soon as reasonably practicable after discovery of the incident will introduce significant pressure on companies to quickly resolve doubts in favor of materiality and disclosure, perhaps even before all facts are conclusively known. Public companies should take steps now to strengthen their disclosure controls and procedures so they can make timely assessments of the materiality of cybersecurity incidents and determine what, if any, disclosure is required. Finally, if adopted without change, the compressed time frame in the Proposed Rules for assessing materiality will reinforce the critical importance of conducting exercises before an incident occurs to ensure that new or amended procedures are well drawn and will work in practice.

As a related matter, if public companies have not previously updated their insider trading policies to capture cybersecurity incidents as potential material nonpublic information, they should do so now. We note that if the Commission adopts its recently proposed amendments to Rule 10b5-1 and related matters, companies will be required to provide disclosure about their insider trading policies. In light of the Commission's and investors' current areas of focus, we anticipate that companies will want to be in a position to disclose that their insider trading policies do indeed address cybersecurity incidents.

In her dissenting statement, SEC Commissioner Hester Peirce voiced concern with the proposed requirement that companies report cybersecurity incidents regardless of investigations that may be conducted by federal and state governments. We expect comments will echo her concern as disclosure may negatively affect a company's or a law

enforcement agency's ability to investigate wrongdoing or recover stolen funds. The SEC acknowledged this risk in the release of the Proposed Rules, but has concluded on balance that the benefits of timely disclosure to investors outweighs these considerations, even if, under state laws, public reporting or notification could be delayed if reporting would impede a civil or criminal investigation.

Additionally, the requirement to disclose both the name of any director with cybersecurity expertise and the nature of the expertise will likely have ramifications in board composition and training practices. In effect, the requirement to disclose board cybersecurity expertise is a substantive requirement that one or some board members have this expertise. Boards will likely seek to add directors with cybersecurity qualifications, but there may not be a significant pool from which to appoint such directors. As a result, boards may instead need to expend additional resources to train their existing members in cybersecurity-related matters in response to the Proposed Rules.

New York
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

London
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com

[1] If a triggering determination occurs within four business days before a registrant's filing of a Form 10-Q or Form 10-K, the Commission staff generally has not objected to the registrant satisfying its Form 8-K reporting obligation by including the disclosure in Item 5 (Other Information) of Part II of its Form 10-Q or Item 9B (Other Information) of its Form 10-K. *See* SEC Division of Corporation Finance, Exchange Act Form 8-K Compliance and Disclosure Interpretations (updated Dec. 22, 2017), Question 1, available at https://www.sec.gov/divisions/corpfin/form8kfaq.htm.