ALSTON & BIRD

WWW.ALSTON.COM

Securities Law / Securities Litigation / Privacy, Cyber & Data Strategy
ADVISORY ■

MARCH 15, 2022

SEC Proposes Sweeping New Cybersecurity Disclosure Rules for Public Companies

by **David A. Brown, Katherine Doty Hanniford, Kimberly Kiefer Peretti, Cara M. Peterman, Rebecca R. Valentino, Alysa Austin, Sierra Shear, *and* Kezia Osunsade**

On March 9, 2022, the Securities and Exchange Commission (SEC) released the latest in a series of proposed rules aimed at bolstering the cybersecurity-related disclosures of regulated entities, this time directed at public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934, as amended. If enacted, the sweeping new rules would require covered public companies to, among other things:

- Report material cybersecurity incidents on Form 8-K within four business days of a materiality determination.
- Routinely update investors on such incidents in quarterly and annual reports.
- Analyze whether individually immaterial cybersecurity incidents are material in the aggregate and report those in quarterly and annual reports.
- Make periodic disclosures regarding the company's cyber-related risk management policies and procedures.
- Periodically disclose cyber-related governance information, including the board's oversight and management's implementation of cyber-related risk management policies and procedures.
- Make periodic disclosures regarding board-level expertise in cybersecurity.

The proposed rules are subject to public comment, to be submitted by May 9, 2022 or 30 days from publication in the *Federal Register*, whichever is later.

Reporting Material Cybersecurity Incidents on Form 8-K

The proposed rules would add new Item 1.05 to Form 8-K and require public companies to disclose certain information within four business days after the company determines that it has experienced a material

cybersecurity incident, which may be different from the date of initial discovery of a cybersecurity incident.

If the proposed rules are adopted, companies would be required to disclose the following information about a material cybersecurity incident, to the extent known, in an initial Form 8-K filing:

- When the incident was discovered and 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 unauthorized purpose.
- The effect of the incident on the company's operations.
- Whether the company has remediated or is currently remediating the incident.

According to the SEC, reporting companies are not expected to "publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." Additionally, under the rules as proposed, an untimely filing of a Form 8-K regarding new Item 1.05 would not result in the loss of Form S-3 eligibility, so long as the company is current in its reporting at the time the Form S-3 is filed.

Significantly, if adopted in its current form, the four-day reporting timeframe would not be extended if there is a law enforcement delay or an ongoing investigation related to the cybersecurity incident. Although the SEC acknowledges that state data breach notification statutes provide exemptions to applicable notification deadlines due to law enforcement or other ongoing investigation considerations, and that a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident, the proposing release described the need for investors to have access to material information as an overriding consideration in this context.

The SEC also recognized that its proposed reporting regime for notice content and timing would be in addition to other potential notification obligations public companies may also be subject to.

Relevant definitions

Materiality

The determination of "materiality" would be consistent with the well-established principles under securities laws; that is, if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available." Building on the standards set forth in the SEC's 2018 guidance and recent enforcement actions involving the sufficiency of disclosure controls following a cyber-incident, companies would be required to "thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances … including both quantitative and qualitative factors," yet also render a materiality

determination "as soon as reasonably practicable after discovery of the incident."

Cybersecurity incident

The proposed rules would introduce a new definition of "cybersecurity incident": "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."

Information systems

The proposed rules further define "information systems" to broadly include "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of a registrant's information to maintain or support the registrant's operation."

Requirement to Provide Updates on Material Cybersecurity Incidents

Under the SEC's proposed amendments to Regulation S-K, companies would be required to provide material updates on any material cybersecurity incident that was previously reported on Form 8-K in the Form 10-Q or Form 10-K covering the period when the material change or update occurred.

Such updates would include any material additional information that was not included in the initial Form 8-K regarding:

- The breadth of the cybersecurity incident.
- Whether any data was compromised.
- The present and future impact of the cybersecurity incident on the company's business.
- Present or future measures to remediate the cybersecurity incident.
- Any changes in the company's policies or procedures as a result of the cybersecurity incident.
- Other material updates.

Reporting of Individually Immaterial Incidents When Material in the Aggregate

Additionally, the proposed amendments would require companies to analyze the materiality of cybersecurity incidents individually and in the aggregate. When incidents that are immaterial individually become material collectively, companies would be required to disclose, in the Form 10-Q or Form 10-K covering the period when the materiality determination is made:

- When the cybersecurity incidents were discovered.
- Whether the incidents are ongoing.
- A description of the incidents.
- Whether the incidents allowed any data to be compromised.
- The impacts of the incidents on the company's business and actions.

- Whether the company has remediated the incidents.

New Cybersecurity Risk Management Disclosure Requirements

The SEC is also proposing to modify Regulation S-K to require companies to periodically disclose information about their policies and procedures on cybersecurity risk management, including whether the company:

- Has a cybersecurity risk assessment program (and, if so, provide a description of the cybersecurity risk program).
- Uses third parties in connection with their cybersecurity risk program.
- Has policies to identify cybersecurity risks with third-party providers.
- Has contractual provisions and other mechanisms to limit cybersecurity risks with third-party providers.
- Has taken steps to prevent and mitigate the effects of cybersecurity incidents.
- Has continuity and recovery plans in place for a cybersecurity incident.
- Has changed company policies due to prior cybersecurity incidents.
- Has experienced impacts on its operations or finances due to cybersecurity risks and incidents (and, if so, describe how the company was impacted).
- Considers cybersecurity risks as a part of the company's business strategy and financial planning.

These disclosures would be made in the company's annual report on Form 10-K.

New Cybersecurity Governance Disclosure Requirements

Additional proposed rule modifications to Regulation S-K would require companies to periodically disclose additional information related to the oversight of cybersecurity risks by the board of directors and management, if cybersecurity risks are material to the company's business. The disclosures for board oversight would include:

- Which directors are responsible for the oversight of cybersecurity risks.
- How the board is informed about cybersecurity risks.
- How frequently the board discusses cybersecurity risks.
- How the board considers cybersecurity risks as a part of the company's business strategy.

Companies would also be required to describe management's relationship with the company's cybersecurity, including:

- Which management positions or committees are responsible for managing the company's cybersecurity risk and the qualifications of those responsible.
- Whether the company has a chief information security officer (or someone in a similar position) and who that individual reports to in the company.
- How the responsible managers and committees monitor and remain informed about cybersecurity incidents and threats.

- How frequently the responsible individuals report to the board on cybersecurity risks.

New Board-Level Expertise Disclosure Requirements

Finally, the proposed rules would amend Item 407 of Regulation S-K to require disclosures for the "cybersecurity expertise" of members of the board (if any). While the rules do not define what constitutes cybersecurity expertise, they provide a nonexhaustive list of criteria that should be considered in determining whether any director has such expertise, including:

- The directors' prior work experience.
- The directors' certifications or degrees in cyber.
- Whether the directors have other relevant knowledge, skills, or other background in cyber.

If any member of the board is determined to have "cybersecurity expertise," the registrant would be required to disclose the names of such directors and "provide such detail as necessary to fully describe the nature of the expertise." The disclosure would be required in the registrant's annual report on Form 10-K and in any proxy or information statement when action is to be taken on director elections.

Looking Ahead

Alston & Bird will continue to monitor the impact of the public comment period on the proposed rules. Nevertheless, given the recent trend to accelerate public comment and implementation periods under Chairman Gary Gensler and because these proposed rules were initially scheduled for release in October 2021, the SEC may move quickly to finalize the proposed rules in some form upon the expiration of the comment period. Accordingly, public companies that are subject to the reporting requirements of the 1934 Act would be well-served by reviewing and updating as appropriate their incident response plans to include decision points for enhanced SEC reporting, as well as to lay the groundwork with boards and management to come into compliance with the more formalized risk management and disclosure measures proposed in the rules.

You can subscribe to future advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you would like more information, please feel free to contact one of the attorneys in our **Securities Group**, **Securities Litigation Group**, **Privacy, Cyber & Data Strategy Group**

.

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor, Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333