FACT SHEET

Public Company Cybersecurity; Proposed Rules

The Securities and Exchange Commission proposed rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies ("registrants") that are subject to the reporting requirements of the Securities Exchange Act of 1934.

Specifically, the proposal would:

- Require current reporting about material cybersecurity incidents on Form 8-K;
- Require periodic disclosures regarding, among other things:
  - A registrant's policies and procedures to identify and manage cybersecurity risks;
  - Management's role in implementing cybersecurity policies and procedures;
  - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
  - Updates about previously reported material cybersecurity incidents; and
- Require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

Background and Current Requirement

In 2011, the Division of Corporation Finance issued interpretive guidance providing the Division's views concerning registrants' existing disclosure obligations relating to cybersecurity risks and incidents. In 2018, the Commission issued interpretive guidance to reinforce and expand upon the 2011 staff guidance. The Commission addressed the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity. Although registrants' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since then, disclosure practices are inconsistent.

The proposed amendments are designed to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents. Consistent, comparable, and decision-useful disclosures would allow investors to evaluate registrants' exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents.

Incident Disclosure Proposed Amendments

The SEC proposed to:

- Amend Form 8-K to require registrants to disclose information about a material cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident;
- Add new Item 106(d) of Regulation S-K and Item 16J(d) of Form 20-F to require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate; and
- Amend Form 6-K to add "cybersecurity incidents" as a reporting topic.

Risk Management, Strategy, and Governance Disclosure

In addition to incident reporting, the SEC proposed to require enhanced and standardized disclosure on registrants' cybersecurity risk management, strategy, and governance. Specifically, the proposal would:

- Add Item 106 to Regulation S-K and Item 16J of Form 20-F to require a registrant to:
    - Describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity as part of its business strategy, financial planning, and capital allocation; and
    - Require disclosure about the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the registrant's cybersecurity policies, procedures, and strategies.
- Amend Item 407 of Regulation S-K and Form 20-F to require disclosure regarding board member cybersecurity expertise. Proposed Item 407(j) would require disclosure in annual reports and certain proxy filings if any member of the registrant's board of directors has expertise in cybersecurity, including the name(s) of any such director(s) and any detail necessary to fully describe the nature of the expertise.

Additional Information:

The public comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.

FACT SHEET

Cybersecurity Risk Management

The Securities and Exchange Commission proposed new cybersecurity risk management rules and amendments to enhance cybersecurity preparedness and improve the resilience of investment advisers and investment companies against cybersecurity threats and attacks.

Specifically, the proposal would:

- Require advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks;
- Require advisers to report significant cybersecurity incidents to the Commission on proposed Form ADV-C;
- Enhance adviser and fund disclosures related to cybersecurity risks and incidents; and
- Require advisers and funds to maintain, make, and retain certain cybersecurity-related books and records.

Background

Advisers and funds play an important role in our financial markets and increasingly depend on technology for critical business operations. Advisers and funds are exposed to and rely on a broad array of interconnected systems and networks, both directly and through service providers such as custodians, brokers, dealers, pricing services, and other technology vendors. As a result, they face numerous cybersecurity risks and may experience cybersecurity incidents that can cause or be exacerbated by critical system or process failures.

The proposed rules and amendments are designed to address concerns about advisers' and funds' cybersecurity preparedness and reduce cybersecurity-related risks to clients and investors; improve adviser and fund disclosures about their cybersecurity risks and incidents; and enhance the Commission's ability to assess systemic risks and oversee advisers and funds.

Proposed Amendments

Cybersecurity Risk Management Rules

The proposal includes new rule 206(4)-9 under the Advisers Act and new rule 38a-2 under the Investment Company Act (collectively, the "proposed cybersecurity risk management rules"). The proposed cybersecurity risk management rules would require advisers and funds to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks. The proposed rules list certain general elements that advisers

Also available as part of the eCourse
2022 Government Enforcement eConference

First appeared as part of the conference materials for the
8th Annual Government Enforcement Institute session
"Cybersecurity and Ransomware: Updates and Best Practices"