ALM | LAW.COM

New York Law Journal

The Year of Cyber Disclosures: Navigating the SEC's New Rules

By Olivia J. Greer, Catherine Kim and Jeeyoon Chung

April 2, 2024

In December of 2020, SolarWinds Corp. publicly acknowledged a major cyberattack that resulted in supply chain compromise and headline discussions about national security and data security. On Oct. 20, 2023 the U.S. Securities and Exchange Commission (SEC or Commission) charged SolarWinds and its chief information security officer (CISO) with fraud for allegedly failing to disclose known material cybersecurity risks and vulnerabilities.

While the complaint references the cyberattack, the lawsuit notably focuses more on SolarWinds' allegedly "poor cybersecurity practices" and lack of internal controls, and, for the first time, implicates a CISO personally.

The SolarWinds complaint came amidst an ongoing trend of SEC cybersecurity-related enforcement, such as charges brought in 2019 against First American Title Insurance Company, and in 2021 against various broker-dealers and investment advisers, all focused on purported failures to implement adequate cybersecurity controls and procedures and, in particular, deficiencies in internal reporting.

Alongside its active enforcement, the SEC has been considering new rules and amendments regarding cybersecurity practices and related reporting requirements. With the first of these rules effective as of Dec. 18, 2023, for public companies, and the landscape of ongoing scrutiny and enforcement, SEC registrants should not lose time in reviewing their cybersecurity postures and policies to ensure compliance and, even ahead of formal adoption of certain still-pending rules, align with best practices.

New and Proposed Rules

A. Public Company Rule

On July 26, 2023, the SEC adopted final rules imposing obligations on public companies regarding

cybersecurity risk management, strategy, governance, and incident disclosure ("Public Company Rule").

Under the new rules, public companies (and foreign private issuers) must annually report their cybersecurity risk management processes, and both management and board oversight of cybersecurity risks, each in sufficient detail for a reasonable investor to understand.

They must also report any "material" cybersecurity incidents within four business days of the company's determination of materiality, and describe the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the business.

The SEC has subsequently clarified that this disclosure requirement should not be read to require companies in the midst of an incident to disclose information that would expose them to further risk or provide bad actors with a roadmap.

B. Two Proposals for Investment Advisers, Investment Companies and Broker-Dealers:

The Commission is also considering rulemaking that would impact broker-dealers, registered investment

advisers, and investment companies, with proposed revisions to Regulation S-P (which imposes certain privacy and cybersecurity requirements on financial institutions under the Gramm-Leach-Bliley Act) and proposed rules under the Investment Advisers Act and the Investment Company Act.

With apparent overlap between the two sets of proposed rules and amendments, it is not yet clear whether the Commission will adopt both and, if so, whether revisions will be made to clarify the overlapping areas. However, based on the Commission's December 2023 update to its rulemaking agenda ("Reg Flex Agenda"), both sets are in the Final Rule stage and appear to be slated for adoption in April 2024.

1. Proposed Regulation S-P Amendments

The SEC's proposed amendments to Regulation S-P, if adopted, will impose new detailed requirements governing how covered entities (*i.e.*, brokers, dealers, investment companies, and investment advisors) protect customer information. These include providing notice of data breaches impacting sensitive customer information to impacted individuals within *thirty days* of discovery.

Amendments to the Safeguards Rule and Disposal Rule under Regulation S-P would also require covered entities to adopt a written incident response program with specified elements, such as certain record retention periods, disclosures in third party agreements, and special considerations for remote work arrangements.

The Safeguards and Disposal Rules would also become applicable to all customer and consumer information that a covered entity possesses, maintains or receives, regardless of whether such information relates to the covered entity's own customers or to customers of other financial institutions, and would expand the applicability of the rules to certain transfer agents.

2. Proposed Registered Investment Advisors and Private Fund Advisers Rule

The SEC's proposed cybersecurity rules and amendments under the Advisers Act will, if adopted, apply to registered investment advisers, private fund advisers and other investment advisers that would not otherwise be required to register with the SEC (*e.g.*, state registrants).

Some of the proposed requirements are shared amongst all organizations that come within the rule's scope, and some relating to reporting and retention have nuances that are specific to either funds or advisers.

Broadly, these rules would require registered investment advisers and investment companies to (i) implement written cybersecurity policies and procedures that are reasonably designed to address cybersecurity risks; (ii) create and maintain certain cybersecurity-related books and records; and, perhaps most notably, (iii) report "significant" cybersecurity incidents to the SEC *within 48 hours* of a determination that the incident is "significant" via a newly-proposed Form ADV-C.

The proposed rules would also enhance required cybersecurity-related disclosures, including amending Form ADV Part 2A (the brochure) to require disclosure of cybersecurity risks and incidents.

C. Additional Proposed Rulemaking

The SEC has proposed several additional cybersecurity rules. A proposed rule under the Advisers Act would require registered investment advisers to conduct due diligence prior to outsourcing certain services—including cybersecurity—and subsequently carry out periodic monitoring of service providers' performance.

Another proposed rule and amendments to existing recordkeeping rules would require broker-dealers, transfer agents, clearing agencies, and certain securities-based entities to disclose significant cybersecurity incidents. And proposed amendments to Regulation Systems Compliance and Integrity (SCI) would expand the reach obligations related to cybersecurity and vendor management to broker-dealers exceeding a certain transaction activity threshold, additional clearing agencies, and security-based swap data repositories.

Based on the Reg Flex Agenda, each of these proposals appears to be in the Final Rule stage and slated for adoption in April 2024.

Key Takeaways

The SEC has not yet released any comment letters critiquing filings under the new Public Company Rule, and the relatively few responsive filings thus far have significantly varied in specificity and detail. Some filings have involved the potential or actual exposure of sensitive personal information of customers, such as social security numbers or driver's license numbers.

Thus far, most of the disclosures appear to include high-level descriptions of specific cybersecurity incidents and processes and, in many cases, state only that certain cybersecurity policies and procedures are in place, rather than describing them.

Recognizing that this is a dynamically evolving area, with best practices and requirements potentially changing rapidly, companies navigating this enforcement and statutory landscape should consider the following takeaways.

• **Disclosure of Material Cybersecurity Incidents.** The SEC has advised that, in determining the "materiality" of a cybersecurity incident, a registrant should consider whether there is a substantial likelihood that a reasonable shareholder would consider the information as important or as having significantly altered the

total mix of information made available. Companies should holistically evaluate the quantitative (*e.g.*, damages) and qualitative (*e.g.*, reputational harm, possibility of regulatory action, etc.) facts and circumstances surrounding an incident. Companies will need to do advance planning to ensure they have the ability to quickly conduct a materiality assessment (and, likely, to do so in an ongoing manner over the course of an incident); establish the participating individuals (including from legal, compliance, management and, where applicable, the board); review and update incident response plans to include assessment and reporting strategies; and identify external advisers in advance.

Since the adoption of the Public Company Rule, some companies have preemptively disclosed cybersecurity incidents even before determining materiality and stated in their filings that their investigation and remediation efforts are ongoing.

Notably, relevant filings have been mostly filed by companies handling the processing of large volumes of, and/or more sensitive, customer information. This suggests that companies are considering the types and volume of potentially affected information when determining materiality.

The proposed Advisers Act amendments include a threshold requirement that the disclosed incident is "significant," which is similar, but not identical to, to the "materiality" standard in the Public Company Rule. Advisers will be able to draw from the examples of disclosures by public companies to guide approach but they will need to solve for the nuances of the different standards.

• **Governance.** Accounting for disclosure requirements concerning the roles and experience of members of management and the board will require companies to ensure that such individuals have appropriate knowledge of cybersecurity policies and procedures, as well as their role and responsibilities with respect thereto.

Companies should ensure that there are clear lines of reporting within the organization, and that relevant parties' roles and experience are sufficiently documented. A number of companies that had not discussed cybersecurity governance in their 2022 filings alongside disclosure of actual or potential cybersecurity incidents, did, in their most recent filings, disclose information about their cybersecurity governance, including, for example, a Chief Information Security Officer's qualifications and the role of the board with respect to cybersecurity risks and incidents.

• **Cybersecurity Policies and Procedures.** Companies should review and update their internal data protection and information security policies and procedures, and, specifically, their incident response plans to ensure incidents are properly documented, investigated, assessed, and potentially reported. Consider incorporating frameworks for assessing materiality within an incident response plan, so that it becomes an automatic part of incident response.

Since the adoption of the Public Company Rule, companies have publicly disclosed general references to their incident response and business continuity plans and, in connection with disclosed incidents, broad descriptions of affected internal systems (*e.g.*, "internal bank network", "IT infrastructure and applications").

• **Scope of Disclosures.** For all of the discussed reporting requirements, companies will need to balance disclosing information sufficient to meet reporting requirements while avoiding unintentionally over-divulging information that may expose the company's cybersecurity profile to cyberattackers.

In the SolarWinds complaint, the SEC largely focused on SolarWinds' failure to disclose specifically known risk factors and noted that the company's SEC filings (which long preceded the new Public Company Rule) included generic and hypothetical risk disclosures.

The SEC has increasingly emphasized the importance of carefully reviewing risk factors to ensure risks are described as actual, as opposed to hypothetical. If a company experiences a cybersecurity incident, disclosures of potential risk factors in the event of a hypothetical cybersecurity incident would be insufficient to satisfy a company's reporting obligations.

Conclusion

The intersection of the cyber-risk landscape and the SEC's rulemaking became explosive in November 2023, when ransomware crime syndicate, ALPHV/BlackCat, filed a whistleblower complaint with the SEC against MeridianLink. After MeridianLink declined to engage with the hackers' demands, ALPHV/BlackCat submitted a complaint alleging that MeridianLink had failed to report the "material" cybersecurity incident perpetrated by ALPHV/BlackCat itself.

The SEC has yet to acknowledge such complaint, but it's clear that the intersection between cyber-risk and SEC rulemaking is a dynamic one and that we can expect the fireworks to continue.

Olivia J. Greer *is a partner at Weil Gotshal & Manges in the firm's technology & IP transactions practice. She is also a member of the firm's privacy & cybersecurity group and AI task force.* **Catherine Kim** *is counsel and* **Jeeyoon Chung** *is an associate in the firm's technology & IP transactions practice.*

Reprinted with permission from the April 2, 2024 edition of the NEW YORK LAW JOURNAL © 2024 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or asset-and-logo-licensing@alm.com. # NYLJ-4032024-55544