

Strategic Perspectives | Cybersecurity Policy Report

SEC Continues Focus On AI And Cyber-Risk Related Enforcement Cases

By [Brendan Quigley](#) and [Matthew R. Baker](#) of [Baker Botts](#)

The SEC kicked off its fiscal year by bringing enforcement actions focused on AI and cyber disclosures. As discussed in more detail below:

- These actions again show SEC Enforcement prioritizing “hot button” issues like AI and cyber, highlighting, for example, a company’s statements about its use of AI in what otherwise appeared to be a fairly garden-variety securities fraud case.
- The actions largely involve well-worn principles of securities law applied in the context of emerging technologies, including (i) while there may be no obligation to speak on a particular issue (such as AI), if a company does speak, its statements must be full, complete, and not misleading and (ii) companies’ obligation to consider whether existing disclosures need to be updated in light of recent events (such as a cyberattack).
- The cyber-disclosure actions prompted a lengthy, two-commissioner dissent, accusing the commission of playing “Monday morning quarterback” by bringing the case, highlighting the potential for the upcoming election (and the appointment of commissioners under a new administration) to impact the SEC’s enforcement posture.
- The dissent in the cyber cases also undertook a lengthy analysis, comparing the allegations in the settled cases to allegations against another company, arising out of the same series of cyberattacks, in an action the SEC litigated in federal district court. As we discussed here and as pointed out by

the dissent, the federal district court dismissed many of those allegations. While deciding to settle with the SEC (or any government agency) is always a complicated, multi-faceted decision, the dissent’s comparison of the litigated case and the settled actions shows the need for parties under investigation to seriously consider the merits of potentially litigating cases when appropriate.

I. Cyber Disclosure Actions

On October 22, 2024, the SEC announced it had reached settlements with four technology companies concerning their cybersecurity-risk related disclosures to investors. Each of the settlements arose out of the companies’ use of Orion software, sold by SolarWinds Corporation, which was the subject of a sophisticated and widespread series of cyberattacks in 2019 and 2020. The attacks targeted not only SolarWinds but other users of the software. The SEC alleged that each of four companies—Unisys, Avaya, Mimecast, and Check Point—were users of the software and negligently minimized their cybersecurity risks and the impact of cybersecurity attacks by the same “threat actor,” believed to be a Russian-intelligence backed hacker. While each of the four cases had different facts, several overarching themes can be gleaned from the SEC’s actions:

- **Companies must be careful to avoid using generic or hypothetical terms to describe cybersecurity risks, when those risks have in fact materialized.** In both

the Unisys and Check Point settlements, the SEC faulted the companies because their investor disclosures used hypothetical or generic terms to describe cybersecurity risks, despite knowing a successful attack had occurred. For example, Unisys issued two 10-Ks stating that cyberattacks “could” result in losses or unauthorized disclosures of the company’s information, and the company “could ...experience data loss [and] impediments to our ability to conduct our business,” even though it knew at the time the “threat actor” had in fact seriously compromised its systems.

- **Companies must consider updating their cybersecurity disclosures following an intrusion.** In both Unisys and CheckPoint settlements, the SEC noted that the companies’ annual SEC filings contained cybersecurity risk factor disclosures that were “virtually” or “substantially” “unchanged” from prior filings, despite the discovery of the Orion compromise.
- **Disclosures around cybersecurity incidents must include the full extent of the breach, to the extent known.** Another major theme, particularly in the Avaya and Mimecast settlements, was that the companies’ investor disclosures minimized the full extent—both in qualitative and quantitative terms—of the cybersecurity compromises.
- For example, while Mimecast issued a Form 8-K after learning its systems had

been compromised, the 8-K stated the attack “target[ed] only a small number of customers,” even though the threat actor had accessed a database containing, according to the SEC, “tens of thousands of customers’ credentials.” While Mimecast also disclosed that the threat actor had accessed a “limited number” of “source code repositories,” it allegedly omitted telling investors that the three source codes accessed were “important to the security of Mimecast’s overall service offering,” and thus to its “ability to protect information” and “ability to attract customers” as a global provider of cloud security. Similarly, Avaya issued a 10-Q stating the compromise had accessed only “a limited number of ... email messages” but had not accessed our “other internal systems.” While these statements were literally true, the SEC noted that Avaya omitted that the email box accessed belonged “cybersecurity personnel” and that, although certain systems accessed were technically not “internal” because they were operated by an outside vendor, Avaya used those systems to store documents and information in the ordinary course of business.

- Finally, the SEC noted in the Avaya and Mimecast settlements that the companies failed to disclose the compromise was likely attributable to a “nation-state threat actor,” which heightened its significance.
- **Importance of maintaining disclosure controls and procedures around cyber.** The SEC also alleged that, in addition to making materially misleading statements around cyber risks, Unisys also failed to maintain adequate disclosure controls and procedures around cybersecurity. In particular, the SEC alleged that Unisys did not require escalation of potentially material incidents to senior management

and “disclosure decision-makers,” i.e., those in management responsible for deciding whether the matter needed to be disclosed to investors.

- **Importance of cooperation and remediation.** In each of the settlements, the SEC cited the companies’ cooperation and remediation, including the companies making lengthy and detailed presentations and summarizing factual issues and information, as well as updating disclosure policies and procedures.

Notably, the Commission was not unanimous. Two commissioners, Mark Uyeda and Hester Peirce, issued a lengthy dissent, accusing the Commission of playing “Monday morning quarterback” with the companies’ cyber disclosures following the sophisticated SolarWinds attack. Commissioners Uyeda and Peirce argued “The Commission needs to start treating companies subject to cyberattacks as victims of a crime, rather than perpetrators of one.” The dissent further noted that in July 2024, in the litigated action against SolarWinds itself, and as we discussed [here](#), a judge in the Southern District of New York **dismissed** much of the SEC’s case, rejecting in particular many of the SEC’s allegations regarding SolarWinds’ own post-Sunburst attack disclosures and rejecting entirely the SEC’s theories about internal accounting controls. The dissent undertook a lengthy analysis comparing the allegations against the four companies in the settled actions to the ones rejected by the court the SolarWinds case, concluding that many of these allegations would not have been material if the action had been litigated in federal district court.

II. “AI-Washing” Action

The SEC also continued to target alleged misrepresentations about the use of artificial intelligence by regulated entities. On October 10, the SEC announced a settlement With

Rimar Capital, LLC, an investment adviser; Rimar USA, its sole owner; its sole employee; and one of its directors.

The SEC alleged that Rimar USA offered securities ostensibly to develop the Rimar LLC platform. The SEC asserted that this offering was, frankly, a fairly garden-variety securities fraud: the offering materials contained numerous misrepresentations, including misrepresenting Rimar LLC’s assets under management; claiming Rimar LLC was set up as a “hedge fund” when it wasn’t; and making misleading claims about past performance. The SEC’s order also noted that “the marketing materials and solicitation communications also repeatedly referred to Rimar LLC as having an artificial intelligence-driven platform for trading, among other products, stock and crypto assets. But the firm had no trading application at all at the time of the fundraising” The agency’s official press release also emphasized the AI-aspect of the alleged fraud, highlighting the case was allegedly about “Defrauding Investors by Making False and Misleading Statements About Use of Artificial Intelligence.”

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Mr. Brendan Quigley
Baker Botts
910 Louisiana Street
Houston, Texas
77002-4995
UNITED STATES
Tel: 713 229 1234
Fax: 713 229 1522
E-mail: bobby.bitner@bakerbotts.com

(c) Mondaq Ltd, 2024 - Tel. +44 (0)20 8544 8300 - <http://www.mondaq.com>