ALERT MEMORANDUM

SEC Charges Four Companies Impacted by Data Breach with Misleading Cyber Disclosures

October 31, 2024

On October 22, 2024, the SEC announced settled enforcement actions charging four companies with making materially misleading disclosures regarding cybersecurity risks and intrusions. These cases mark the first to bring charges against companies who were downstream victims of the well-known cyber-attack on software company SolarWinds. The four companies were providers of IT services and digital communications products and settled the charges for amounts ranging from $990,000 to $4 million.

In 2023, the SEC sued SolarWinds and its Chief Information Security Officer for allegedly misleading disclosures and deficient controls. Most of the SEC's claims in that case were dismissed by a judge in the Southern District of New York, in part because the judge ruled that SolarWinds' post-incident disclosures did not misleadingly minimize the severity of the intrusion. This new round of charges indicates the SEC's intent to continue to enforce disclosure and reporting requirements surrounding cybersecurity breaches. The SEC's recent charges focus on the companies' continued use of generic and hypothetical language following significant data breaches, as well as allegations of downplaying the severity of the breaches by omitting material information about their nature and extent. Public companies should carefully consider the lessons from these actions when making disclosures following a cybersecurity breach.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Francesca Odell
+1 212 225 2530
flodell@cgsh.com

Helena Grannis
+1 212 225 2376
hgrannis@cgsh.com

Lillian Tsu
+1 212 225 2130
ltsu@cgsh.com

Ryken Kreps
+1 212 225 2317
rkreps@cgsh.com

WASHINGTON

Tom Bednar
+1 202 974 1836
tbednar@cgsh.com

Background

According to the SEC's allegations, which the companies neither admitted nor denied, in December 2020, each of the four companies charged last week learned that its systems had been affected by the SolarWinds data breach. Public reporting at the time indicated that the breach was likely performed by a state-sponsored threat actor. Each of the companies performed investigations of the breach, determining that the threat actor had been active in their systems for some period of time and accessed certain company or customer information.[1]

The SEC brought negligent fraud charges against all four companies, charging two primary types of materially misleading disclosures. Two companies, Check Point[2] and Unisys,[3] were charged because the SEC believed their post-breach risk factor disclosures—containing generic and hypothetical language about the risk of cybersecurity breaches similar to their *pre*-breach disclosures—were misleading given that the companies had become aware of the actual SolarWinds-related breaches. The SEC alleged that the other two companies, Avaya[4] and Mimecast,[5] while they did make specific disclosures that they had been affected by cybersecurity breaches, misleadingly omitted details that the SEC asserted would be material to investors. The SEC noted that all four companies were in the information technology industry, with large private and government customers, and therefore their reputation and ability to attract and retain customers would be affected by disclosure of a data breach.

The Charges

There were two categories of charges.

Charges for disclosing hypothetical cyber risks in wake of actual cyber attack. The SEC has repeatedly brought charges against companies for allegedly using generic and/or hypothetical language in their risk factors after a known data breach.[6] That trend has continued with the recent actions against Check Point and Unisys.

i. Check Point

Check Point's Form 20-F disclosures in 2021 and 2022 stated, "We regularly face attempts by others to gain unauthorized access…" and "[f]rom time to time we encounter intrusions or attempts at gaining unauthorized access to our products and network. To date, none have resulted in any material adverse impact to our business or operations."[7] These filings were virtually unchanged before and after the data breach. The SEC alleged that these risk disclosures were materially misleading because the company's risk profile materially changed as a result of the SolarWinds compromise-related activity for two reasons: the threat actor was likely a nation-state and the threat actor "persisted in the network unmonitored for several months and took steps, including deployment and removal of unauthorized software and attempting to move laterally" in the company's environment.[8]

[1] For information on the four orders, *See* Press Release, *SEC Charges Four Companies With Misleading Cyber Disclosures*, SEC, https://www.sec.gov/newsroom/press-releases/2024-174.
[2] Check Point Software Technologies Ltd., Securities Act Release No. 11321, Exchange Act release No. 101399, SEC File No. 3-22270 (Oct. 22, 2024).
[3] Unisys Corporation, Securities Act Release No. 11323, Exchange Act Release No. 101401, SEC File No. 3-22272 (Oct. 22, 2024).
[4] Avaya Holdings Corp., Securities Act Release No. 11320, Exchange Act Release No. 101398, SEC File No. 3-22269 (Oct. 22, 2024).
[5] Mimecast Limited, Securities Act Release No. 11322, Exchange Act Release No. 101400, SEC File No. 3-22271 (Oct 22, 2024).
[6] Press Release, *Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million*, SEC, https://www.sec.gov/newsroom/press-releases/2018-71; Press Release, *SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors*, SEC, https://www.sec.gov/newsroom/press-releases/2023-48.
[7] Check Point, *supra* note 2, at 2–4.
[8] *Id.*

ii. Unisys

The company's risk factors in its Form 10-Ks following the breach were substantially unchanged from 2019. The risk factor language was hypothetical: cyberattacks "could … result in the loss … or the unauthorized disclosure or misuse of information…" and "*if* our systems are accessed …."[9] The SEC alleged that hypothetical language is insufficient when the company is aware that a material breach occurred. The SEC also alleged that the company did not maintain adequate disclosure controls and procedures because they had no procedures to ensure that, in the event of a known cybersecurity incident, information was escalated to senior management, which in this case did not happen for several months. The SEC's order also alleged that the company's investigative process after the breach "suffered from gaps that prevented it from identifying the full scope of the compromise," and that these gaps constituted a material change to the company's risk profile that should have been disclosed.[10]

Charges for allegedly failing to disclose material information. Two of the charged companies did disclose that their systems had been affected by suspicious activity, but the SEC nevertheless found fault with those disclosures.

i. Avaya

In its Form 10-Q filed two months after learning of the breach, the company disclosed that it was investigating suspicious activity that it "believed resulted in unauthorized access to our email system," with evidence of access to a "limited number of Company email messages."[11] The SEC alleged that these statements were materially misleading because they "minimized the compromise and omitted material facts" that were known to the company "regarding the scope and potential impact of the incident,"[12] namely, omitting: (i) that the intrusions were likely the work of a state actor, and (ii) that the company had only been able to access 44 of the 145 files compromised by the threat actor and therefore could not determine whether these additional files contained sensitive information.[13]

ii. Mimecast

In its Form 8-Ks filed in the months after learning of the breach, Mimecast disclosed that an authentication certificate had been compromised by a sophisticated threat actor, that a small number of customers were targeted, that the incident was related to SolarWinds, and that some of the company's source code had been downloaded. The company stated that the code was "incomplete and would be insufficient to build and run" any aspect of the company's service.[14] The SEC alleged that these statements were materially misleading "by providing quantification regarding certain aspects of the compromise but not disclosing additional material information on the scope and impact of the incident," such as the fact that the threat actor had accessed a database containing encrypted credentials for some 31,000 customers and another database with systems and configuration information for 17,000 customers, and by not disclosing that the threat actor had exported source code amounting to more than half of the source code of the affected projects, or information about the importance of that code.[15]

Dissenting Statement

The two Republican Commissioners, Hester Peirce and Mark Uyeda, voted against the actions and issued a dissenting statement accusing the Commission of "playing Monday morning quarterback."[16] The dissenters noted two key issues across the orders. First, the dissenters viewed the cases as requiring disclosure of details about the cybersecurity incident itself, despite previous Commission statements that

[9] Unisys Corporation, *supra* note 3, at 6.
[10] *Id.* at 5–7.
[11] Avaya Holdings Corp, *supra* note 4, at 4.
[12] *Id.* at 2.
[13] *Id.* at 4.
[14] Mimecast Limited, *supra* note 5, at 4.
[15] *Id.*
[16] Statement, Comm'rs Peirce and Uyeda, *Statement Regarding Administrative Proceedings Against SolarWinds Customers* (Oct. 22, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224.

disclosures should instead be focused on the "impact" of the incident.[17] Second, the dissenters argued that many of the statements the SEC alleged to be material would not be material to the reasonable investor, such as the specific percentage of code exfiltrated by the threat actor.[18]

The SEC Is Not Backing Off After *SolarWinds*

These enforcement actions come months after the Southern District of New York rejected several claims the SEC brought against SolarWinds for the original breach.[19] The recent actions show that the SEC is not backing away from aggressively reviewing incident and other related cybersecurity disclosures. Notably, the SEC did not allege that any of the companies' cybersecurity practices violated the Exchange Act's internal controls provision. In an issue of first impression, the *SolarWinds* court held that the internal controls provisions focus on *accounting* controls and do not encompass the kind of cyber defenses at issue in that case. It is not clear whether the absence of such charges here represents the SEC adopting a new position after the *SolarWinds* ruling, or rather a reflection of these cases involving different cybersecurity and intrusions. The SEC did allege failure to maintain proper disclosure controls in one of the four new orders, which was another allegation rejected by the *SolarWinds* court as insufficiently pled.[20] Moreover, the *SolarWinds* court dismissed claims that the company had misled its investors by making incomplete disclosures after its cyber intrusion, finding that the company adequately conveyed the severity of the intrusion and that any alleged omissions were not material or misleading. While the dissenters questioned whether the allegedly misleading disclosures here were any different than those in *SolarWinds*, at a minimum these cases show that the SEC will continue to closely scrutinize post-incident disclosures, notwithstanding its loss in *SolarWinds.*

Takeaways

There are several takeaways from these charges.

- The SEC is signaling an aggressive enforcement environment and continuing to bring claims against companies for deficient disclosure controls, despite similar charges being rejected in *SolarWinds*. The Unisys order shows that the SEC will continue to pursue disclosure controls charges where, in its view, a company did not adequately escalate incidents to management, consider the aggregate impact of related incidents, or adopt procedures to guide materiality determinations, among other things.
- The SEC will reliably bring charges against companies that use generic or hypothetical risk factor language to describe the threat of cybersecurity incidents when the company's "risk profile changed materially"[21] due to a known breach.
- The SEC will give heightened scrutiny to disclosures by companies in sectors such as information technology and data security, because in the SEC's view cybersecurity breaches are more likely to affect the reputation and ability to attract customers for these types of companies.
- Companies should take care in crafting disclosures about the potential impact of cybersecurity breaches, including in Form 8-K and risk factor disclosure, and consider factors such as:
    - Whether the threat actor is likely affiliated with a nation-state.

[17] *Id.*

[18] *Id.*

[19] *See* Cleary Alert Memo, *SDNY Court Dismisses Several SEC Claims Against SolarWinds and its CISO* (July 26, 2024).

[20] *Id.*

[21] Unisys Corporation, *supra* note 3, at 5.

- Whether, or the extent to which, the threat actor persisted in the company's environment.
- If the company seeks to quantify the impact of the intrusion, such as by the number of files or customers affected, the SEC will scrutinize whether the company selectively disclosed quantitative information in a misleading way.
- Whether the company should disclose not only the number of files or amount customer data compromised, but the importance of the files or data and the uses that can be made of them.
- If the company quantifies the impact of the intrusion but is aware of gaps in its investigation or in the available data that mean the severity of the impact could have been worse, the SEC may consider it misleading not to disclose those facts.

…

CLEARY GOTTLIEB