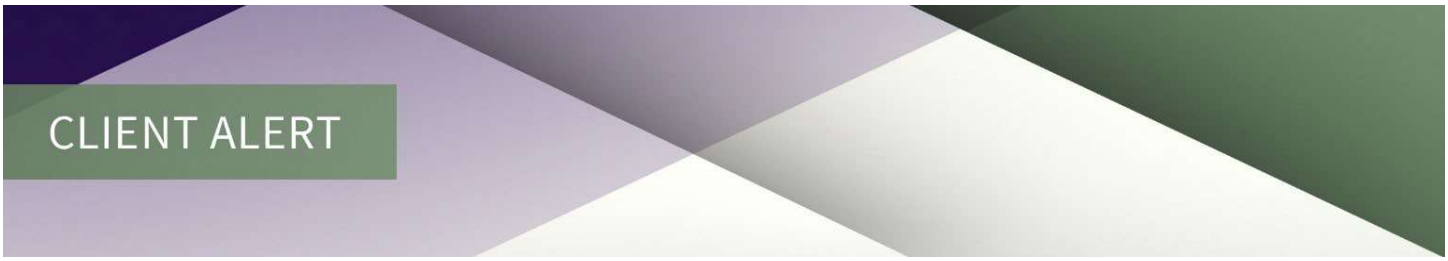
WILLKIE FARR & GALLAGHER LLP



The SEC Settles Enforcement Actions with Four Companies for Cyber Disclosure Failures

October 29, 2024

AUTHORS

Laura E. Jehl | Daniel K. Alvarez | A. Kristina Littman | Adam S. Aderton

Marc J. Lederer

On October 22, 2024, the U.S. Securities and Exchange Commission ("Commission" or "SEC") announced it had settled enforcement actions with four current or former public companies (the "Respondents[1]") for making materially misleading disclosures regarding cybersecurity risks and intrusions.[2] The charges brought by the SEC stemmed from an investigation involving public companies potentially impacted by the SolarWinds Orion software compromise. [3] The SEC found that the threat actor likely behind the SolarWinds Orion incident had accessed the Respondents' systems without authorization, and that each of these companies negligently minimized the extent of its cybersecurity compromise in its public disclosures. In general, the SEC found these companies' cyber disclosures to be generic or hypothetical, and thus misleading in light of the facts in these cases. The Commission also charged one of the Respondents (Unisys) with related controls violations.

These actions are notable for several reasons. First, while the SEC has historically taken the position that cyber risk disclosures are misleading if they characterize cyber risks as hypothetical in the face of actual incidents, one new action goes further. As noted below, the SEC's order against Check Point found that a risk disclosure was misleading because it was generic and not tailored to the company's risks, notwithstanding the risk disclosure explicitly indicating that the

1 The Respondents are as follows: Avaya Holdings Corp., Check Point Software Technologies Ltd. and Mimecast Limited, Unisys Corporation

2 Press Release, *SEC Charges Four Companies With Misleading Cyber Disclosures*, U.S. SECURITIES AND EXCHANGE COMMISSION (October 22, 2024) available at https://www.sec.gov/newsroom/press-releases/2024-174?utm_medium=email&utm_source=govdelivery.

3 For more information regarding the Solar Winds data breach and the SEC's response to the data breach, see, Court Dismisses SEC's Novel Cybersecurity Claim Against SolarWinds (July 25, 2024), https://www.willkie.com/-/media/files/publications/2024/07/court-dismisses-sec-s-novel-cybersecurity-claim-against-solarwinds.pdf/.

company is routinely targeted and that periodically intrusions are successful, but that none had resulted in a materially adverse impact. Second, several of the orders scrutinize the level of detail or materiality determinations made by the Respondents when they made specific disclosures about the incident. The SEC's order against Avaya notes that the company disclosed the investigation into its compromise in a periodic filing, but the SEC disagreed with Avaya's determination that the incident was not material. The SEC's order against Mimecast notes that the company filed multiple Forms 8-K disclosing details of the compromise, but the Commission found this deficient because the disclosures described some details but not others.

SolarWinds's Background

On December 14 and 17, 2020, SolarWinds, a U.S. software company whose products are widely used to manage IT networks, systems, and infrastructure, disclosed in SEC filings that a targeted cyberattack[4] had inserted a vulnerability into its centralized IT monitoring and management software, Orion. SolarWinds stated that up to 18,000 customer-installed Orion products might be affected by the vulnerability, which had been inadvertently delivered as an update to SolarWinds's Orion software ("SolarWinds Compromise").

In the Matter of Unisys Corporation

Misleading Filings

Unisys is a global provider of technical and enterprise information technology services to a variety of private and public organizations.

In December 2020, Unisys first identified an infected version of the Orion software on at least one computer in its network.[5] On December 13, 2020, Unisys's then senior cybersecurity personnel received credible information that likely the same threat actor had compromised Unisys's network and non-customer-facing cloud environment using means other than SolarWinds's software beginning in February 2020. The company's subsequent investigation uncovered evidence that the threat actor engaged in a number of malicious activities, including compromising and gaining access to a number of user and employee accounts and transferring a large amount of data from the company's network.

Unisys filed with the SEC annual reports on Form 10-K for fiscal years ended December 31, 2020 and 2021 that included cybersecurity risk disclosures that described the existence of successful intrusions and the risk of unauthorized access to data and information in hypothetical terms. The SEC found that these disclosures were materially misleading because Unisys knew that the intrusions were not hypothetical but instead had actually happened, and involved unauthorized access and exfiltration of confidential and/or proprietary information.

[4] The threat actor behind the compromise of the SolarWinds Orion software was a hacking group likely associated with a nation-state.

[5] Securities and Exchange Commission, In the Matter of Unisys Corporation, Exchange Act Release No. 101401, October 22, 2024.

The SEC determined that Unisys had violated a number of rules and regulations:

- Section 17(a)(2) of the Securities Act of 1933 ("Securities Act"), which prohibits making untrue or misleading statements, in the offer or sale of a security;
- Section 17(a)(3) of the Securities Act, which makes it unlawful for any person in the offer or sale of a security to engage "in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser";
- Section 13(a) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 13a-1 thereunder, which require issuers of a security registered pursuant to Section 12 of the Exchange Act to file with the Commission annual reports in conformity with the Commission's rules and regulations; and
- Rule 12b-20 of the Exchange Act, which, among other things, requires such issuers to include in annual reports filed with the Commission any material information necessary to make the required statements in the filing not misleading.

Failure to Maintain Disclosure Controls and Procedures

Unisys's cybersecurity personnel failed to report all their findings regarding the security compromises that took place in 2020 and 2021 to their disclosure decision-makers for a year after they were discovered. Their cybersecurity personnel also failed to report a separate extortion incident that occurred in 2022 until the hackers made a public statement. The SEC found that, at the time of these events, Unisys did not maintain effective controls requiring escalation of potentially material incidents to senior management and disclosure decision-makers. The SEC also noted that Unisys did not have controls and procedures designed to ensure that its disclosure decision-makers reviewed cybersecurity incident information in Unisys's possession to determine which information about the incident might require disclosure in Commission filings. Accordingly, Unisys failed to maintain disclosure controls and procedures designed to ensure that information related to material cybersecurity incidents was, among other things, reported to management responsible for disclosures and therefore timely reported to investors. Lastly, the SEC found that Unisys's deficient controls contributed to Unisys's materially misleading risk factor disclosures for the years ending 2020 and 2021.

The SEC concluded that Unisys violated Exchange Act Rule 13a-15(a), which requires issuers with a security registered pursuant to Section 12 of the Exchange Act to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms.

Unisys agreed to pay $4,000,000 as a civil money penalty and to cease and desist from further violations.

In the Matter of Mimecast Limited

Mimecast is a provider of cloud security and risk management services for email and corporate information.

The SEC Settles Enforcement Actions with Four Companies for Cyber Disclosure Failures

In January 2021, Mimecast learned that its systems had been compromised by the same threat actor that was responsible for the SolarWinds Compromise.[6] The threat actor had accessed internal emails, an encrypted database and server and configuration information for thousands of customers ("Mimecast Compromise").

In early 2021, Mimecast publicly disclosed certain aspects of the Mimecast Compromise through a number of Forms 8-K filed with the Commission. However, the SEC found that Mimecast negligently omitted a number of material aspects of the Mimecast Compromise, including information regarding the large number of impacted customers and the percentage of code exfiltrated by the threat actor. The SEC further determined that Mimecast negligently created a materially misleading picture of the Mimecast Compromise by providing quantification regarding certain aspects of its compromise but not disclosing additional material information on the scope and impact of the incident. Adding to the overall materiality of the omissions, the SEC noted that "Mimecast is a global provider of cloud security and risk management services for email and corporate information, and its data and code were of great interest to state-sponsored cyber threat actors. In addition, due to Mimecast's services, its ability to protect information and data stored on and transmitted over its systems was critically important to its reputation and ability to attract customers."[7]

As a result of these filings, which the SEC deemed misleading, the SEC concluded that Mimecast violated Section 17(a)(2) and Section 17(a)(3) of the Securities Act as well as Section 13(a) of the Exchange Act and Rule 13a-11 thereunder. Finally, the SEC found that Mimecast had violated Rule 12b-20 of the Exchange Act.

Mimecast agreed to pay $990,000 as a civil money penalty and to cease and desist from further violations.

In the Matter of Check Point Software Technologies Ltd.

Check Point developed, marketed, and supported a wide range of products and services for IT security by providing an architecture meant to defend enterprises' cloud, network, and mobile devices.

On December 14, 2020, Check Point identified instances of infected SolarWinds's installations on two Check Point servers.[8] Check Point then learned that the malicious activity in the Check Point environment related to the SolarWinds Compromise occurred during a four-month period from July through October 2020, and that, in addition to the two infected servers, the unauthorized activity included the installation and use of unauthorized software, compromise of two corporate accounts, and network reconnaissance and attempted lateral movement.

6 Securities and Exchange Commission, In the Matter of Mimecast Limited, Exchange Act Release No. 101400, October 22, 2024.

7 Id. p. 5.

8 Securities and Exchange Commission, In the Matter of Check Point Software Technologies Ltd., Exchange Act Release No. 101399, October 22, 2024.

The SEC found that Check Point's disclosures in its 2021 Form 20-F and 2022 Form 20-F were materially misleading because they omitted new and material cybersecurity risks arising out of the SolarWinds Compromise.

In addition to being inaccurate, the SEC determined that Check Point's 2021 and 2022 cybersecurity risk disclosures were generic and not tailored to the company's "particular cybersecurity risks and incidents" which created a materially misleading impression of the cybersecurity risks Check Point faced and understood post-incident. "These disclosures were also materially misleading by framing any intrusion as not material, by generally stating that Check Point 'encounter[s] intrusions or attempts at gaining unauthorized access,' but that none have had a "materially adverse impact."[9]

The SEC seemed particularly troubled by the omission that a likely nation-state threat actor was present and unmonitored in Check Point's network. Furthermore, the SEC order noted that Check Point's omissions were also material because Check Point's business involved providing IT security services and that protecting its networks and data was critically important to its reputation and ability to attract customers.

As a result of these misleading filings, the SEC concluded that Check Point violated Section 17(a)(2) and Section 17(a)(3) of the Securities Act as well as Section 13(a) of the Exchange Act and Rule 13a-11 thereunder. Finally, the SEC found that Check Point had violated Rule 12b-20 of the Exchange Act.

Check Point agreed to pay $995,000 as a civil money penalty and to cease and desist from further violations.

In the Matter of Avaya Holdings Corp.

Avaya is a provider of digital communication products, software, and services for businesses, including large multinational enterprises, and governments in the United States and abroad.

On December 15, 2020, Avaya first learned that software infected by the SolarWinds Compromise had allowed unauthorized activity by the threat actor on the affected servers and on its network.[10] Avaya later learned that the threat actor had compromised Avaya's cloud email and file-sharing environment using means other than SolarWinds's software.

The SEC found that Avaya was negligent in making materially misleading statements in its 10-Q filed on February 9, 2021, as it omitted material facts known to Avaya personnel regarding the scope and potential impact of its compromise. Specifically, Avaya omitted the likely attribution of the compromise to a nation-state threat actor, the long-term unmonitored presence of the threat actor in Avaya's systems, the access to at least 145 shared files some of which contained confidential and/or proprietary information, and the fact that the mailbox the threat actor accessed belonged to one of Avaya's cybersecurity personnel. The SEC also found Avaya was negligent in including in the February 2021 disclosure a statement

[9] Id. P. 5.

[10] Securities and Exchange Commission, In the Matter of Avaya Holdings Corp., Exchange Act Release No. 11320, October 22, 2024.

that there was "no current evidence" of access to "our other internal systems," which was misleading for omitting the fact that Avaya was aware of the threat actor's access to at least 145 shared files in the cloud file-sharing environment.

The SEC also noted that Avaya never publicly made any statements or disclosure that corrected the negligently made material misstatements and omissions described above.

The SEC concluded that Avaya violated Section 17(a)(2) and Section 17(a)(3) of the Securities Act as well as Section 13(a) of the Exchange Act and Rule 13a-13 thereunder. Finally, the SEC found that Avaya had violated Rule 12b-20 of the Exchange Act.

Avaya agreed to pay $1,000,000 as a civil money penalty and to cease and desist from further violations.

Dissenting Opinion

In a dissenting opinion, Commissioners Hester M. Peirce and Mark T. Uyeda (the "Dissent") disagreed with the Commission's conclusions in these cases and believed that bringing these actions did more harm than good for investors.[11]

Much of the dissenting opinion centered on the Commission's view on what a reasonable investor would view as material in reading each of the Respondents' disclosures. For instance, the Dissent did not think the identity of the threat actor would be material to investors and did not think that many of the details that were omitted by the Respondents would be material. Instead, the Dissent believed that the impact of the incident –as opposed to the details– was what would be material to investors. Indeed, they contended that a filing is not misleading if the disclosure, read as a whole, captures the big picture. The Dissent was instead worried about excessive disclosure of immaterial events, in which it stated, "aggressive enforcement by the Commission may cause companies to fill their risk disclosures with occurrences of immaterial events, for fear of being second-guessed by the Commission. Such a result would frustrate the Commission's goal of preventing a lengthy risk factor section filled with immaterial disclosure."

Final Thoughts

These cases show how closely the SEC is scrutinizing firms' responses to cybersecurity incidents and the Commission's view of materiality as it relates to a data breach. These enforcement actions make clear the SEC's view that cyber disclosures contained in public company filings should not be worded generally or hypothetically, particularly when a company has experienced a cyber incident. The SEC is telling firms to tailor their cyber disclosures to their own particular cybersecurity risks and incidents they experience. The SEC also expects such disclosures not to omit material information

[11] Statement of Commissioners Hester M. Peirce and Mark T. Uyeda, *Statement Regarding Administrative Proceedings Against SolarWinds Customers,* U.S. SECURITIES AND EXCHANGE COMMISSION (Oct. 22, 2024), available Here.

or make material misstatements in order to minimize the effect of a cyber incident. As stated by Jorge G. Tenreiro, Acting Chief of the Crypto Assets and Cyber Unit, "Downplaying the extent of a material cybersecurity breach is a bad strategy."[12]

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

A. Kristina Littman
202 303 1209
aklittman@willkie.com

Adam S. Aderton
202 303 1224
aaderton@willkie.com

Marc J. Lederer
212 728 8624
mlederer@willkie.com

[12] Press Release, *SEC Charges Four Companies With Misleading Cyber Disclosures*, U.S. SECURITIES AND EXCHANGE COMMISSION (October 22, 2024) available at https://www.sec.gov/newsroom/press-releases/2024-174?utm_medium=email&utm_source=govdelivery.