SEC Charges Four Companies for Misleading Cyber Disclosures

October 28, 2024

On October 22, 2024, the U.S. Securities and Exchange Commission (the "SEC") announced settled charges in separate actions against four technology companies—Avaya Holdings Corp. ("Avaya"), Check Point Software Technologies Ltd. ("Check Point"), Mimecast Limited ("Mimecast"), and Unisys Corp. ("Unisys")—each of which was a downstream victim of the unprecedented 2020 cyber-attack in which threat actors believed to be state-sponsored hackers in Russia inserted malware called SUNBURST (the "SUNBURST malware") into a SolarWinds software update (the "SUNBURST attack").

According to the SEC's Orders (the "Orders"), all four companies had, unknowingly installed the SUNBURST malware prior to the public announcement of the SUNBURST attack in 2020, and all four were ultimately compromised by the perpetrators of that attack. The SEC alleged that each company made materially misleading cybersecurity-related statements or omissions related to these events, in violation of Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 (the "Securities Act") and Section 13(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), as well as various rules thereunder. The Commission also charged Unisys with violations of the Exchange Act's disclosure controls and procedures provision. While neither admitting nor denying the findings in the Orders, each company agreed to pay a penalty of between $990,000 and $4 million. Commissioners Peirce and Uyeda issued a lengthy joint dissenting statement in which they raised multiple criticisms of the resolutions, and emphasized that, "donning a Monday morning quarterback's jersey to insist that immaterial information be disclosed — as the Commission did in today's four proceedings — does not protect investors."

In June 2024, Judge Engelmayer dismissed nearly all of the SEC's claims against SolarWinds and its now-CISO. The October 22, 2024 actions represent the SEC's first resolutions based on its multi-year investigations into the adequacy and accuracy of disclosures made by the downstream victims of the SUNBURST attack. Although the disclosures and statements at issue in these four matters pre-date the SEC's new cybersecurity disclosure rules, companies should closely consider these cases as

reflecting the Commission's latest views on materiality assessments and disclosure decisions regarding cybersecurity incidents.

The Four Orders

The four companies charged by the Commission are alleged to have certain common attributes: all were public technology or software companies (although two, Avaya and Mimecast, have since been taken private); all had installed at least one instance of the SUNBURST malware; and all experienced SUNBURST-related intrusions between at least 2020 and 2021 by the Russian nation-state threat actors (the "Threat Actors") who were responsible for the SUNBURST attack. The SEC alleged that all four negligently made materially misleading statements in light of their victimization. In explaining the materiality of the incidents, the SEC emphasized the nature of the respondents' businesses, noting that, as IT service and software providers, the circumstances of the attacks would have been "critically important" for, e.g., the companies' reputations, customers, and investors. Because the details of the breaches and disclosure issues were quite different in each order, we recount below the different fact patterns described in the four Orders.

The Avaya Order

According to the *Avaya* Order, in December 2020, Avaya, a global provider of digital communications products, software and services, identified two servers segmented from its corporate network that had installations of the SUNBURST malware. The malware made initial connections to a server controlled by the Threat Actors, but apparently did nothing more. However, according to the Order, in December 2020, Avaya was separately notified by a third-party service provider that "likely the same" Threat Actors had compromised Avaya's external cloud email and file sharing environment using means other than the SUNBURST malware. The Threat Actors accessed 145 files—44 of which Avaya was able to recover and review, including some with confidential and proprietary information (such as security procedures and passwords)—and monitored an email account of one of Avaya's cybersecurity incident response personnel. According to the Order, Avaya determined that the initial unauthorized activity occurred in January 2020 and the last known activity occurred in December 2020.

In February 2021, Avaya disclosed in its Form 10-Q that it was investigating suspicious activity that it believed resulted in a breach with "evidence of access to a limited number of Company email messages." The Form 10-Q stated that Avaya had not identified "current evidence of unauthorized access to [its] other internal systems," and the incident had not materially adversely impacted its business or operations.

The SEC found that Avaya was negligent in making these statements, which allegedly contained material misstatements and omissions about the severity of the incident and its potential implications. Specifically, the SEC found that the Form 10-Q failed to disclose: the likely attribution to the known Threat Actors; the long-term presence of the Threat Actors in Avaya's systems; the access to the 145 files, including some with confidential information; and the fact that the Threat Actors accessed the mailbox of one of Avaya's cybersecurity personnel. The Order also found that, in light of the compromise of the external file-sharing environment, Avaya had been negligent in stating that there was "no current evidence" of access to "our other internal systems." While the Order conceded that the file-sharing environment "was not technically 'internal' to Avaya," the SEC alleged that the statement was misleading because "Avaya used that environment to store its documents and information in the ordinary course of business."

Although Avaya had filed a Form 10-Q in May 2022, stating that some of "the attacks [had] been sponsored by state actors with significant financial and technological means," the SEC alleged that this did not correct the earlier misstatements about the scope of the compromise.

While neither admitting nor denying the findings in the Order, Avaya agreed to pay a $1 million penalty in connection with the settlement.

The Check Point Order

According to the SEC, in December 2020, Check Point, an IT security company, identified instances of the SUNBURST malware on two of its servers. Shortly thereafter, a third party notified Check Point of potential unauthorized activity related to the SUNBURST attack in its environment. Check Point's subsequent investigation revealed that the unauthorized activity occurred between July and October 2020, and that, in addition to the two servers with SUNBURST malware installed, the unauthorized activity included the installation and use of unauthorized software typically associated with malicious data exfiltration, network reconnaissance and attempted lateral movement within the network environment. The SEC alleged that Check Point's investigation was unable to identify the full scope of the compromise because many of its logs of network and internet activity were limited to September through December 2020. Check Point's investigation did not identify evidence that any customer data, code, or other sensitive information was accessed.

According to the SEC, Check Point's April 2021 and April 2022 annual reports framed the company's cybersecurity risks "generically" and without sufficient tailoring to address the company's "particular risks . . . and incidents." These risk disclosures were identical to those of prior years despite the allegedly material change to Check Point's

cybersecurity risks as a result of the SUNBURST attack. The Form 20-F filings stated that "[w]e regularly face attempts . . . to gain unauthorized access through the Internet or to introduce malicious software to our . . . systems," that "malicious hackers may attempt to gain unauthorized access," and that "[t]o date, [no attempts to gain unauthorized access] have resulted in any material adverse impact to our business or operations."

The SEC found that Check Point had negligently made disclosures that were materially misleading insofar as they omitted how the company's cybersecurity risks had increased due to the SUNBURST attack and the limits of the company's ability to assess the scope of activity prior to September 2020. The SEC also found materially misleading the use of generic statements that were not tailored to the cybersecurity risks that the company faced and understood post-incident. Finally, the SEC found that it was materially misleading for the company to frame any intrusions it had experienced as not material.

While neither admitting nor denying the findings in the Order, Check Point agreed to pay a $995,000 penalty in connection with the settlement.

The Mimecast Order

According to the SEC, in December 2020, Mimecast, a cloud security and risk management services provider, identified computers in its network with instances of the SUNBURST malware. The next month, Mimecast discovered that the Threat Actors responsible for the SUNBURST attack had accessed internal Mimecast emails and exfiltrated an authentication certificate, substantial portions of Mimecast's source code for certain of its software products, a database containing encrypted credentials for approximately 31,000 customers, and server and configuration information for approximately 17,000 customers. The company's investigation found no evidence that the Threat Actors had accessed relevant decryption keys or accessed customer email or archive data. While Mimecast concluded (after substantial investigation) that the attacks were "related" to the SUNBURST attack, the Order is unclear as to whether the SUNBURST malware was in fact the sole source of the compromise experienced by the company.

From January through March 2021, Mimecast filed a series of Form 8-Ks that, according to the Commission, included material misstatements or omissions related to these events. For example, Mimecast's disclosures had included quantifying information regarding the "small" or "low single digit" number of customers that had been targeted by means of the stolen certificate and the "limited number of . . . source code repositories" that had been exfiltrated. The disclosures further stated that the exfiltrated source code was "incomplete and would be insufficient to build and run any aspect of the Mimecast service."

The SEC found that these statements were materially misleading as to the scale of the compromise and that they omitted material information, including: (i) that the Threat Actors had gained access to the credentials for the majority of Mimecast's customers; and (ii) that while the exfiltrated code was "a small portion of Mimecast's complete product code," "the functions it served were important to the security of Mimecast's overall service offering." The SEC found also that Mimecast had misleadingly omitted the fact that the Threat Actors had exfiltrated 58% of a certain source code, 50% of Mimecast's Microsoft 365 authentication source code, and 76% of its Microsoft 365 interoperability source code. The SEC alleged that, together, these disclosures had negligently created a "materially misleading picture" by providing quantifiable information related to certain aspects of the cybersecurity incident, but not disclosing additional material information on the scope and impact of the incident.

While neither admitting nor denying the findings in the Order, Mimecast agreed to pay a $990,000 penalty in connection with the settlement.

The Unisys Order

According to the *Unisys* Order, in December 2020, Unisys, a global provider of technical and information technology services and solutions, identified one computer on its network with the SUNBURST malware installed. Unisys later learned, after an investigation, that two other computers had each connected once to a known malicious command-and-control server.

Unisys eventually received credible information that the Threat Actors behind the SUNBURST attack had compromised its network and non-customer facing cloud environment (using means other than the SUNBURST malware) beginning in February 2020. Its subsequent investigation showed that, for extensive periods in 2020 through 2021, the Threat Actors infiltrated its systems, gained access to network credentials and compromised user accounts (including accounts with global administrative privileges and other accounts used for customer service), exfiltrated gigabytes of data, and accessed at least five cloud-based mailboxes (including those of senior IT personnel).

In August 2021, Unisys again received credible information, which was not reported to senior management, that the same Threat Actors had accessed the company's VPN and non-customer facing environment earlier that year. The subsequent investigation identified evidence of persistent unauthorized activity, compromised user accounts, unauthorized access to 14 systems, unauthorized VPN sessions, and access to thousands of emails and files. The Threat Actors allegedly carried out this attack using information obtained in the 2020 attack.

The SEC alleged that the Unisys annual reports for 2020 and 2021 "negligently framed" the company's risk factors related to cybersecurity events as hypothetical, despite Unisys's awareness of the 2020 SUNBURST attack-related compromise of its environment. The reports stated that the cyberattacks "could . . . result in the loss . . . or unauthorized disclosure or misuse of company information, and that "[i]f our systems are accessed . . . we could . . . experience data loss and impediments to our ability to conduct our business, and damage the market's perception of our services and products" (emphasis omitted). The SEC alleged that, although Unisys's cybersecurity risk profile had "change[d] materially," its disclosures were "substantially unchanged" from those in its 2019 annual report.

The Order goes on to explain that in 2022, Unisys again learned of malware in its network. Failing to apprehend the nature of the attack and believing that it was quarantined, cybersecurity personnel initially designated the attack a low priority. Unisys later learned that the threat was not quarantined and that a criminal ransomware group had exfiltrated code offered to customers. During this event, the company discovered its endpoint detection and response system was not properly configured, and that its related policies and procedures were not followed. In a November 2022 Form 8-K filing, Unisys disclosed a material weakness in its disclosure controls and procedures and its internal controls over financial reporting.

Finally, in 2023, the company learned of another incident involving the same Threat Actors. After an initial investigation based on a third-party tip received in April 2023, Unisys received information from law enforcement in May 2023 that revealed unauthorized access to cloud environments with administrative privileges. As with the August 2021 breach discovery, the Threat Actors were alleged to have used connections likely established in 2020. The Order asserts that the company was unable to fully investigate these incidents due to its limited access to relevant logs and forensic evidence.

Based on these allegations, the SEC found that Unisys negligently made materially misleading statements in Commission filings about the 2020, 2021, and 2022 incidents and violated the Exchange Act's disclosure controls and procedures requirements.

While neither admitting nor denying the findings in the Order, Unisys agreed to pay a $4 million penalty in connection with the settlement.

Dissenting Statement of Peirce and Uyeda

SEC Commissioners Hester Peirce and Mark Uyeda (together, "Dissenting Commissioners") issued a dissenting statement to the settlements, stating that "[r]ather than focusing on whether the companies' disclosure provided material information to investors, the Commission engage[d] in a hindsight review to second-guess the disclosure and cite[d] immaterial, undisclosed details to support its charges."

The Dissenting Commissioners found "troubling" the Commission's conclusion that Avaya negligently omitted disclosure of the threat actor's identity. They argued that the SEC's 2023 cybersecurity rulemaking did not express the view that the identity of the Threat Actors was material, and the absence of comments on this rulemaking requesting this change reflected that investors did not consider the identity of threat actors to be material. Further, they argued that attribution would not have "significantly altered the 'total mix' of information" to a reasonable investor given the highly publicized information surrounding the SUNBURST attack. As to the alleged omitted material information, the Dissenting Commissioners said that it was information about the details regarding the incident—not about the impact of the incident—that the Commission had previously said do not need to be disclosed.

With respect to Mimecast, the Dissenting Commissioners observed that the company did not receive any credit for filing Form 8-K disclosures even though there was no requirement to do so at the time. The Dissenting Commissioners argued that the Mimecast charges incorrectly "focus[ed] on the detail of the threat actor accessing a database containing customer credentials, as opposed to the larger picture of the effects of the incident." The Dissenting Commissioners argued that access to credentials, without more (as was the case with Mimecast) may not be material, and requiring disclosure of precise percentages defies what a reasonable investor would expect. The Dissenting Commissioners expressed concern that the Avaya and Mimecast settlements could lead companies to "fill their Item 1.05 disclosures with immaterial details about an incident, or worse, provide disclosure under the item about immaterial incidents," undermining the benefits and rationale of the Commission's new cybersecurity disclosure requirements.

The Dissenting Commissioners also challenged the SEC's characterization of Check Point's risk factor disclosures as "generic," noting that the federal district court adjudicating the SolarWinds litigation dismissed the SEC's claims brought based on similarly worded disclosures. With respect to the SEC's characterization of Unisys's disclosures as "hypothetical," the Dissenting Commissioners warned that such charges could lead to a proliferation of disclosures of immaterial events by registrants "for fear of being second-guessed by the Commission." The Dissenting Commissioners also

argued that the Commission's other reasons for charging Unisys were unsupported: first, the fact that a "persistent and reportedly nation-state supported threat actor compromised the company's environment" did not necessarily establish materiality; second, the duration of unauthorized access, while concerning, was not necessarily material; and third, the fact that an investigation of an attack suffered deficiencies did not implicate the materiality of the attack itself.

Key Takeaways for Companies

1. **Refresh your risk factors to acknowledge emerging cybersecurity risks and incidents.** By now, virtually every company has been the victim of a cybersecurity attack. Revise and refresh risk factors to reflect emerging cybersecurity risks and actual incidents. Avoid hypothetical descriptions of risks that have materialized.

2. **Ensure that a process exists for coordination between cybersecurity and disclosure personnel during an incident.** The *Unisys* Order confirms that the SEC is prepared to charge alleged disclosure process breakdowns in connection with alleged misstatements and omissions about material cybersecurity events in public filings. Assess your disclosure controls and procedures relating to cybersecurity incidents and ensure that lines of communication between technical and legal personnel, and with disclosure decision makers, are established. Ahead of a real-time cybersecurity crisis, consider running incident response tabletops to test the workflow for the 8-K filing process in connection with potentially material cybersecurity incidents.

3. **Ensure that your cybersecurity 8-K analysis—and disclosures—are comprehensive.** The 8-K analysis for a cybersecurity analysis should address key elements of materiality such as the duration and scope of threat actor access; volume and type of data accessed and/or exfiltrated; and potentially even the identity of the threat actor. Any 8-K disclosures should be carefully crafted to avoid downplaying the severity of the incident and should include sufficient detail about the nature and material impacts of the incident.

4. **Cooperate and remediate.** The Commission has consistently emphasized the importance of cooperation, and its press release announcing the four settlements noted that "[e]ach company cooperated during the investigation, including by voluntarily providing analyses or presentations that helped expedite the staff's investigation and by voluntarily taking steps to enhance its cybersecurity controls." A company faced with an SEC cybersecurity investigation should strongly consider taking actions that will allow it to receive "cooperation credit," which can be

reflected through the Commission's public statements, language in settlement orders, and potential reduction of penalty amounts and other remedies.

5. **Increase your logging capabilities.** The *Unisys* Order found that the company's investigation "suffered from gaps" that prevented the company from understanding the full scope of the cybersecurity incident, and the *Check Point* Order found that the company's limited logging "prevented it from identifying the full scope of the compromise." Enhancing logging capabilities is a prudent step that can improve a company's ability to respond swiftly and comprehensively to a cybersecurity incident—and potentially mitigate any subsequent enforcement interest.

* * *

Please do not hesitate to contact us with any questions.

Andrew J. Ceresney
Partner, New York
+1 212 909 6947
aceresney@debevoise.com

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Benjamin R. Pedersen
Partner, New York
+1 212 909 6121
brpedersen@debevoise.com

Julie M. Riewe
Partner, Washington, D.C.
+1 202 383 8070
jriewe@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
amoody@debevoise.com

Kelly Donoghue
Associate, New York
+1 212 909 6145
kgdonoghue@debevoise.com

Ciera Mandelsberg
Associate, New York
+1 212 909 6961
cmmandelsberg@debevoise.com

Noah L. Schwartz
Associate, New York
+1 212 909 6767
nlschwartz@debevoise.com