JENNER & BLOCK

Key Takeaways from Recent SEC Cybersecurity Enforcement Actions

Client Alerts

October 23, 2024
By: Shoba Pillay, Charles D. Riely, H. Kurt von Moltke, Zoë Higgins Reinstein

The SEC recently announced disclosure settlements against four current and formerly public companies impacted by the highly publicized compromise of SolarWinds' signature network monitoring software, Orion. The settlements generally found that these companies used SolarWinds' Orion software, learned that the threat actor behind the SolarWinds Orion compromise had accessed their systems, and subsequently minimized the cybersecurity incident in their public disclosures. This client alert analyzes the cases and provides key takeaways for public companies.

Background

In 2023, the SEC brought fraud charges against SolarWinds and its CISO in connection with the Orion compromise, and we have covered the developments in this litigation here and here. In relevant part, the SEC alleged that SolarWinds, which provides various information technology management services to customers, overstated the steps it took to prevent cybersecurity incidents and then failed to tell the whole truth after it learned of a massive breach of Orion that impacted many of its key customers. According to public reporting, the SolarWinds' customers impacted by the breach included government agencies such as the Departments of Defense and State and a wide range of private companies.

The SEC's most recent cybersecurity settlements concern some of the customers impacted by the Orion compromise. As described below, the SEC announced disclosure charges against four companies (Unisys, Avaya, Check Point, and Mimecast) with respect to post-incident disclosures that the SEC alleged misled investors by minimizing the scope and nature of the impact of the SolarWinds Orion compromise. Two of the companies—Avaya and Mimecast—disclosed the compromise but omitted certain information about the incident, while the other two companies—Check Point and Unisys—did not update their risk factor disclosures in light of the incident. The below chart summarizes the settlements in descending order of penalties from $4,000,000 to $990,000.

Chart: Summary of the SEC's Most Recent Cybersecurity Settlements

Company	Relevant Disclosures	Charges	Penalty	Cooperation &

				Remediation
Unisys	Post-incident disclosures in the company's Form 10-K described its risks from cybersecurity events as "hypothetical," despite knowing that it had experienced two SolarWinds-related intrusions.	Violation of Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 ("Securities Act"), Section 13(a) of the Securities Exchange Act of 1934 ("Exchange Act"), and Rules 12b-20, 13a-1, and 13a-15(a) thereunder.	$4,000,000	Unisys cooperated in providing the staff with lengthy and detailed presentations, summarizing specific factual issues, and taking steps to remediate its control deficiencies.
Avaya	Post-incident disclosures in the company's Form 10-Q stated that the threat actor accessed a limited number of company emails, without disclosing that the incident also involved access to confidential and/or proprietary information, including third-party application passwords, internal security procedures, instructions regarding remote access, and product configuration information for at least one customer.	Violation of Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20 and 13a-13 thereunder.	$1,000,000	Avaya cooperated in providing the staff analysis and other information, conducting an internal investigation, and taking steps to enhance its cybersecurity controls.
Check Point	Post-incident Form 20-F disclosures described its risks from cybersecurity events in generic terms despite knowing that it had experienced	Violation of Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act,	$995,000	Check Point cooperated in giving the staff detailed explanations, analysis, and

	SolarWinds-related intrusions.	and Rules 12b-20 and 13a-1 thereunder.		summaries, conducting an internal investigation, and taking steps to enhance its cybersecurity controls.
Mimecast	Post-incident Form 8-K disclosures failed to disclose the nature of the code that the threat actor exfiltrated and the quantity of encrypted credentials accessed.	Violation of Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20 and 13a-11 thereunder.	$990,000	Mimecast cooperated with the staff throughout the entirety of the investigation, including giving detailed explanations, analysis, and summaries of multiple specific factual issues, conducting an internal investigation, and taking steps to enhance its cybersecurity controls.

Unisys

Unisys Corp. is a global provider of technical and enterprise IT services and solutions to large commercial enterprises and public sector entities. The SEC order against Unisys found that the company's post-incident disclosures in its Form 10-K for 2020 and 2021 described its risks from cybersecurity events in "hypothetical" terms, despite knowing by December 2020 that it had experienced two SolarWinds-related intrusions starting in January 2020, and intrusions by two additional threat actors between February 2020 and May 2023.

The SEC found that the company had identified the compromise of at least seven network credentials and 34 cloud-based accounts between January and December 2020, as a result of the SolarWinds Orion compromise. This activity included repeated connections into Unisys's network, at

least 23 gigabytes of data transferred, and access to cloud-based shared files and mailboxes of senior IT personnel. Further, between February 2020 and May 2023, a separate threat actor successfully compromised Unisys's network and exfiltrated cybersecurity and product software code. A further incident in July 2022 involved a password-stealing malware, Mimikatz, accessing the company's non-customer-facing software development network.

Without incident response policies that required cybersecurity personnel to report information regarding these incidents to its decisionmakers, Unisys's cybersecurity personnel failed to report these incidents. Further, Unisys knew that its subsequent investigation into these incidents involved significant gaps in its ability to identify the full scope of the unauthorized activity. As a result, its Form 10-K disclosures during this period were not "sufficiently tailored to its particular risks and incidents."

Ultimately, the SEC found that the company failed to maintain disclosure controls and procedures sufficient to ensure that information about material cybersecurity incidents was timely recorded, processed, summarized, and reported to investors. Unisys settled to negligence-based charges pursuant to Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20, 13a-1, and 13a-15(a) thereunder. After taking into account the company's cooperation and remediation, the SEC imposed a $4,000,000 penalty.

Avaya

Avaya Holdings Corp. is a global provider of digital communications products and services for large enterprises and governments. The SEC order against Avaya found that the company's post-incident disclosures in its Form 10-Q filed in February 2021 made materially misleading statements regarding a cyberattack discovered in December 2020 that resulted from the SolarWinds Orion compromise.

The SEC found that the company knew that a threat actor had accessed at least 145 files in its cloud filesharing platform, some of which contained confidential and/or proprietary information, including third-party application passwords, internal security procedures, instructions regarding remote access, and product configuration information for at least one customer. However, its Form 10-Q disclosure omitted this information and only indicated that a threat actor had accessed a limited number of the company's email messages. Avaya never publicly made any statements or disclosures that corrected the "negligently-made material misstatements and omissions."

Avaya settled to negligence-based charges pursuant to Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20 and 13a-13 thereunder. After taking into account the company's cooperation, the SEC imposed a $1,000,000 penalty.

Check Point

Check Point Software Technologies Ltd. provides IT security products and services. The SEC order against Check Point found that the company's post-incident disclosures in its Form 20-F disclosures filed April 2 and April 14, 2022 described cyber intrusions and their risks in generic terms despite the company's knowledge of the Orion compromise.

The SEC found that the company knew that, as a result of the SolarWinds Orion compromise, a threat actor had conducted malicious activity involving two of the company's corporate accounts and had attempted to move laterally into the Check Point environment. Check Point did not believe that the unauthorized activity involved access to customer data, code, or other sensitive information, but Check Point's unauthorized activity logs did not reach back to the start of the intrusion, so the company could not be sure. Despite the company's knowledge of this incident and the subsequent material change in the company's security risk profile, Check Point's Form 20-F disclosures were "virtually unchanged" from its prior disclosures and were not "tailored to the company's particular cybersecurity risks *and incidents*."

Check Point settled to negligence-based charges pursuant to Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20 and 13a-1 thereunder. After taking into account the company's cooperation and remediation, the SEC imposed a $995,000 penalty.

Mimecast

Mimecast Ltd. provides cloud security and risk management services for email and corporate information to approximately 40,000 customers. The SEC order against Mimecast found that the company "negligently made materially misleading misstatements" in its January and March 2021 Form 8-K disclosures regarding a cyberattack discovered in January 2021 by the same threat actor involved in the SolarWinds Orion compromise. These statements to investors minimized the attack by failing to disclose the nature of the code that the threat actor exfiltrated and the quantity of encrypted credentials accessed.

The SEC found that the company knew that a threat actor had exfiltrated a Mimecast-issued authentication certificate used by approximately ten percent of its customers, compromised five customers' cloud platforms using the certificate, and accessed internal email and Mimecast's source code, including a database containing encrypted credentials for approximately 31,000 customers and server configuration information for approximately 17,000 customers. Despite the company's knowledge of this incident, Mimecast's Form 8-K disclosures failed to disclose and downplayed the number of customers impacted, and did not describe that the quantity of source code exfiltrated. This "created a materially misleading picture of the compromise."

Mimecast settled to negligence-based charges pursuant to Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20 and 13a-11 thereunder. After

taking into account the company's remediation and cooperation, the SEC imposed a $990,000 penalty.

Dissenting Statement from Commissioners Hester M. Peirce and Mark T. Uyeda

Commissioners Peirce and Uyeda issued a statement criticizing the settlements and observing at the outset that SolarWinds and its customers were victims of a cyberattack:

> "According to the Government Accountability Office, the 2019-2020 cyberattacks against SolarWinds . . . and its Orion software were "one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and the private sector." It was an attack against America. How has the Commission responded? By first charging SolarWinds in district court and, in today's settled proceedings charging four customers of its Orion software, with violations of the federal securities laws. Today's proceedings impose nearly $7 million in penalties against these victims of the cyberattacks."

The dissenting statement further concluded that the settlements were demonstrative of the SEC "playing Monday morning quarterback" by second-guessing the companies' post-incident disclosures without focusing on whether the disclosures provided material information. Among other things, Commissioners Peirce and Uyeda questioned whether the following disclosures would be material to investors:

- **The identity of the threat actor**. In the Avaya settlement the Order noted that "the likely attribution of the [cyberattack] to a nation-state threat actor" could be material to investors. The dissenting statement noted that the identity of the threat actor, without more, lacked a clear link to the impact of the incident, as required by the SEC's 2023 Cybersecurity Rules, and noted that comment letters during the rulemaking process did not even mention the identity of the threat actor.

- **Specific percentages or amounts of data access by the threat actor.** In the Mimecast settlement, the Order disclosed to investors that the threat actor had accessed encrypted customer credentials and exfiltrated source code, without specifying the percentages or types of source codes. The dissenting statement noted that the disclosures as a whole sufficiently conveyed the whole story about the impact of the incident.

With regard to risk factor disclosures, Commissioners Peirce and Uyeda noted that the Court's ruling in the SolarWinds' motion to dismiss rejected the SEC's position that a company must necessarily update its risk factor disclosures to more specifically address a major cybersecurity incident. In their view, the risk factor disclosures in the Check Point settlement sufficiently alerted investors to the risks that the company faced.

Takeaways

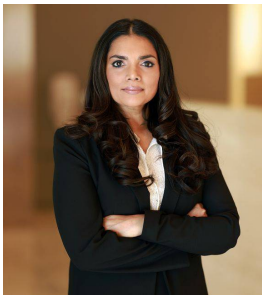
- **Cybersecurity continues to be an enforcement priority for the SEC.** The SEC appears to be pressing ahead with cybersecurity enforcements despite mixed results—most of which were negative for the SEC—in the SolarWinds litigation, as discussed in our prior client alert. With four cybersecurity settlements, the SEC is messaging to public companies that it will continue to scrutinize post-incident disclosures in the wake of a major cybersecurity incident.

- **The SEC's recent cybersecurity settlements reinforce the importance of disclosure and escalation procedures in the wake of a major cybersecurity incident.** The SEC propounded its main disclosure theory in cybersecurity enforcement actions, *i.e.*, that an issuer cannot issue generic cybersecurity risk factor disclosures or statements that could be construed as minimizing a cybersecurity incident if it becomes aware that the incident is severe. The SEC has brought several cybersecurity enforcement actions that conform to this theory, as discussed here.

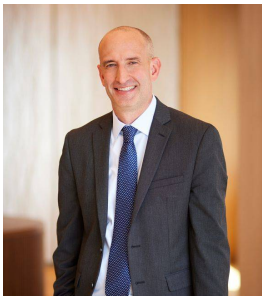
- **The SEC has signaled a willingness to be aggressive on charges and remedies in cybersecurity actions, but the enforcement landscape is uncertain**. The settlements apply a consistent, but aggressive, approach in seeking negligence-based fraud charges (versus standalone disclosure controls charges) and significant penalties despite mitigating factors such as cooperation and remediation. Interestingly, however, the SEC did not pursue pre-incident disclosure theories or other charges, such as internal accounting controls charges, as it has in other cybersecurity enforcement actions. In addition, the dissenting statement from Commissioners Peirce and Uyeda indicates overall caution in bringing cybersecurity enforcement actions and could portend a less aggressive approach in future investigations in the event of a change in administration.

Ultimately, public companies face considerable challenges in making appropriate disclosure decisions in an aggressive SEC enforcement environment while simultaneously dealing with a cybersecurity incident. Companies should ensure that they are prepared—from an incident response and disclosure policy perspective—before a major cybersecurity incident and consult with counsel if faced with difficult disclosure decisions in the event of an incident.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



Charles D. Riely
Partner
criely@jenner.com
+1 212 891 1686

H. Kurt von Moltke
Partner
kvonmoltke@jenner.com
+1 312 840 7499

Zoë Higgins Reinstein
Associate
zreinstein@jenner.com
+1 312 840 7420

Related Capabilities

Data Privacy and Cybersecurity

Investor and Securities Litigation

Stay Informed →