UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 11320 / October 22, 2024

SECURITIES EXCHANGE ACT OF 1934
Release No. 101398 / October 22, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-22269

In the Matter of **Avaya Holdings Corp.,** **Respondent.**	**ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER**

I.

The Securities and Exchange Commission ("Commission") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 8A of the Securities Act of 1933 ("Securities Act") and Section 21C of the Securities Exchange Act of 1934 ("Exchange Act") against Avaya Holdings Corp. ("Avaya" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-And-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds[1] that:

Summary

1. This matter concerns materially misleading statements that Avaya, a global provider of digital communications products and services, negligently made to investors regarding a significant cybersecurity incident that Avaya had experienced. In December 2020, Avaya identified that two servers segmented from Avaya's corporate network had installations of SolarWinds' Orion software, which a likely nation-state threat actor[2] infected with malicious code. The SolarWinds Orion software containing this malicious code allowed for unauthorized activity on affected servers and their networks. This same threat actor separately had compromised Avaya's cloud e-mail and sharing environment as early as January 2020 with activity through at least December 2020. During that timeframe, the threat actor had accessed 145 shared files, some of which contained sensitive company information, and had accessed and monitored a mailbox for one of Avaya's cybersecurity incident response personnel.

2. On February 9, 2021, Avaya filed a report on Form 10-Q with the Commission, which stated 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 … email messages." Avaya was negligent in issuing this materially misleading statement. It minimized the compromise and omitted material facts known to Avaya personnel regarding the scope and potential impact of the incident.

3. Based on the foregoing conduct, and the conduct described herein below, Avaya violated Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20 and 13a-13 thereunder.

Respondent

4. Avaya is a Delaware corporation with headquarters in Morristown, New Jersey. From January 2018 to February 2023, its stock traded on the New York Stock Exchange under the ticker symbol AVYA, and its common stock was registered under Section 12(b) of the Exchange Act. In February 2023, Avaya terminated its registration under the Exchange Act following commencement of a bankruptcy proceeding and acquisition of its common stock by privately-held companies. Between 2018 and 2023, Avaya was required to file with the Commission, among other things, annual reports on Forms 10-K and periodic reports on Forms 10-Q pursuant to Section 13(a) of the Exchange Act and related rules thereunder.

[1] The findings herein are made pursuant to Respondent's Offer and are not binding on any other person or entity in this or any other proceeding.

[2] The term "threat actor" refers to an individual, group, organization, or government that conducts or has the intent to conduct unauthorized activities against the networks and data of or used by others.

Facts

5. At all relevant times, Avaya was a provider of digital communication products, software, and services for businesses, including large multi-national enterprises, and governments in the United States and abroad. Its products and services facilitated its customers' communications and collaboration among their own employees, including technical and professional support, as well as communications with their own customers. As a result, Avaya's information technology networks and resources regularly stored and transmitted its customers' data and information, in addition to Avaya's own data.

6. On December 15, 2020, Avaya identified one server in a separate cloud environment for certain customers and one server in a segregated Avaya development lab network with installations of SolarWinds Orion software, which a persistent threat actor infected with a malicious code that would allow the threat actor to engage in unauthorized activity on the affected servers and on the network in which the servers operated. Both of these installations were segmented from Avaya's corporate network. Avaya's December 2020 investigation identified evidence that the infected software made initial connections to a server controlled by the threat actor, but did not identify evidence of any further activity.

7. Throughout December 2020, Avaya learned that the threat actor behind the compromise of the SolarWinds Orion software was a hacking group likely associated with a nation-state. Public reports and commercial cybersecurity intelligence sources widely attributed the activity to the Russian Federation in late December 2020. On January 5, 2021, a joint public statement by the Federal Bureau of Investigations, the Office of the Director of National Intelligence, the National Security Agency, and the Cybersecurity and Infrastructure Security Agency attributed the attack to an intelligence gathering operation "likely Russian in origin."

8. Also in December 2020, Avaya received notification from a third-party service provider that likely the same threat actor had compromised Avaya's cloud email and file sharing environment using means other than SolarWinds software. Avaya commenced an investigation with the assistance of a third-party forensics services provider in December 2020, and realized that the initial unauthorized activity occurred as early as January 2020 and last known activity occurred in December 2020. Specifically, during its December 2020 investigation, Avaya learned that, in January 2020, the threat actor accessed 145 shared files. Avaya could recover and review 44 of the files. Some of these 44 files contained confidential and/or proprietary information, including third-party application passwords, internal security procedures and information, instructions regarding remote access, and product configuration information for at least one customer. Avaya reviewed the file names and locations of the remaining 101 files, but was unable to recover them or review their content to determine whether the files contained sensitive information. For one of the 44 files, Avaya determined a customer notification was appropriate and, in May 2021, notified the customer associated with the file.

9. By January 2021, Avaya's investigation also discovered that in November and December 2020, the threat actor accessed and monitored a mailbox for one of its cybersecurity incident response personnel. The threat actor was publicly reported to monitor the email traffic of its victims' cybersecurity personnel after compromising an environment, with the apparent goal of

monitoring detection and remediation efforts and adjusting evasion techniques to minimize the likelihood of detection of its activity. Other than the access to the shared files and this mailbox, Avaya's investigation did not identify any evidence of additional unauthorized activity taking place between January and November 2020.

10. On February 9, 2021, Avaya filed its quarterly report on Form 10-Q with the Commission. In the report, Avaya stated that, in the course of its investigation, "which [was] nearing completion," it identified "evidence of access to a limited number of Company email messages" and "no current evidence of unauthorized access to our other internal systems." The filing also stated "we do not believe that this incident has had or will have a material adverse impact on our business or operations." Avaya was negligent in making these materially misleading statements. Avaya was a global digital communications services and software provider to large enterprises and governments, and its data were of great interest to state-sponsored cyber threat actors, such as the threat actor likely at issue here. As a result, due to Avaya's business, its ability to protect information and data stored on and transmitted over its systems was critically important to its reputation and ability to attract and retain customers. Yet, the February 2021 disclosures omitted material information known to Avaya at the time of the filing, including the likely attribution of the activity 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. Avaya was also negligent in including in the February 2021 disclosure a statement 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. Although the cloud file sharing environment was not technically "internal" to Avaya because it was operated by Avaya's vendor, Avaya used that environment to store its documents and information in the ordinary course of business.

11. Throughout the periods discussed above, including following the filing of the February 9, 2021 Form 10-Q, Avaya offered and sold securities to its employees.

12. Avaya never publicly made any statements or disclosure that corrected the negligently-made material misstatements and omissions described above. During the staff's investigation, on May 10, 2022, Avaya filed a quarterly report on Form 10-Q with the Commission, stating that "[i]n come [sic] cases the attacks have been sponsored by state actors with significant financial and technological means." However, this limited additional information did not correct the earlier misstatements regarding the scope of the 2020 compromise involving its cloud email and file sharing environment.

Violations

13. As a result of the conduct described above, Avaya violated Section 17(a)(2) of the Securities Act, which proscribes, in the offer or sale of a security, obtaining "money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading."

14. As a result of the conduct described above, Avaya violated 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."[3]

15. As a result of the conduct described above, Avaya violated Section 13(a) of the Exchange Act and Rule 13a-13 thereunder, which require issuers of a security registered pursuant to Section 12 of the Exchange Act to file with the Commission quarterly reports in conformity with the Commission's rules and regulations. Avaya also violated Rule 12b-20 of the Exchange Act, which, among other things, requires such issuers to include in quarterly reports filed with the Commission any material information necessary to make the required statements in the filing not misleading.

Avaya's Cooperation

16. In determining to accept the Offer, the Commission considered Avaya's voluntary cooperation afforded the Commission staff, including providing the staff with analysis and other information that aided the efficiency of the staff's investigation. In addition, Avaya conducted an internal investigation, shared its findings with the staff on its own initiative, and took certain steps to enhance its cybersecurity controls.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

Accordingly, it is hereby ORDERED that:

A. Pursuant to Section 8A of the Securities Act and Section 21C of the Exchange Act, Respondent cease and desist from committing or causing any violations and any future violations 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.

B. Respondent shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of $1,000,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. §3717. Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

[3] Negligence is sufficient to establish violations of Sections 17(a)(2) and 17(a)(3). *Aaron v. SEC*, 446 U.S. 680, 697 (1980).

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying Avaya Holdings Corp. as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Jorge Tenreiro, Crypto Assets and Cyber Unit, Deputy Chief, Division of Enforcement, Securities and Exchange Commission, Pearl Street, Suite 20-100, New York, NY 10004-2616.

C. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

D. Respondent acknowledges that the Commission is not imposing a civil penalty in excess of $1,000,000 based upon its cooperation in a Commission investigation. If at any time following the entry of the Order, the Division of Enforcement ("Division") obtains information indicating that Respondent knowingly provided materially false or misleading information or materials to the Commission, or in a related proceeding, the Division may, at its sole discretion and with prior notice to the Respondent, petition the Commission to reopen this matter and seek an order directing that the Respondent pay an additional civil penalty, Respondent may contest by way of defense in any resulting administrative proceeding whether it knowingly provided materially false or misleading information, but may not: (1) contest the findings in the Order; or (2) assert any defense to liability or remedy, including, but not limited to, any statute of limitations defense.

By the Commission.

Vanessa A. Countryman
Secretary