UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 11322 / October 22, 2024

SECURITIES EXCHANGE ACT OF 1934
Release No. 101400 / October 22, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-22271

In the Matter of

Mimecast Limited,

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 Mimecast Limited ("Mimecast" 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 misstatements negligently made by Mimecast to investors regarding a cybersecurity incident that Mimecast had experienced. In December 2020, Mimecast identified computers in its network that had installations of SolarWinds' Orion software, a software which a persistent and reportedly nation-state-supported threat actor[2] infected with malicious code that allowed for unauthorized activity on affected computers and their networks. At that time, Mimecast identified no additional unauthorized activity in its systems by the threat actor. In January 2021, Mimecast learned that the same threat actor compromised Mimecast (the "Compromise"). Through the Compromise, the threat actor exfiltrated a Mimecast-issued authentication certificate used by approximately ten percent of its customers and compromised five customers' cloud platforms using the certificate. The threat actor also accessed internal email, certain of Mimecast's source code, including its authentication and data exgestion[3] source code, a database containing encrypted credentials[4] for approximately 31,000 customers, and server and configuration information for approximately 17,000 customers.

2. Mimecast filed Forms 8-K in January 2021 and March 2021 disclosing and discussing the Compromise, including quantifying certain aspects of the Compromise, but negligently failed to disclose the number of customers whose credentials or server and configuration information were accessed by the threat actor. Contemporaneous with the filing of the Forms 8-K, Mimecast began notifying customers impacted by the Compromise.

3. In its March 2021 Form 8-K, Mimecast also disclosed that the threat actor had accessed and downloaded certain source code but did not describe the nature of the code, nor quantify the amount of source code exfiltrated. In fact, the threat actor had accessed and exfiltrated

[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.

[3] "Exgestion" is an internal Mimecast process that converts email data stored in Mimecast's proprietary storage format into an open format for storage or use outside of Mimecast.

[4] The term "credential" refers to a username and password combination or key used to access resources on a network. Compromised credentials are used by threat actors to gain unauthorized access to these resources. Different credentials have varying levels of access to and privileges on the network. For instance, administrative credentials generally have broader access to the network and allow the operator to take actions a standard user would not be able to take, such as adding new credentials or modifying the level of access for existing credentials, among other things. Generally, a threat actor that compromises more credentials and credentials with higher privileges will be more persistent and more difficult to eradicate from a network.

a large percentage of its source code related to exgestion, Microsoft 365 ("M365") authentication, and M365 interoperability code.

4. Based on the foregoing conduct and the conduct described herein below, Mimecast 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-11 thereunder.

Respondent

5. Mimecast was a Jersey corporation headquartered in London, United Kingdom. During the relevant period, Mimecast's stock traded on the Nasdaq Global Select Market under the ticker symbol MIME, and its common stock was registered under Section 12(b) of the Exchange Act. During the relevant period, Mimecast filed with the Commission, among other things, periodic reports on Forms 8-K pursuant to Section 13(a) of the Exchange Act and Rule 13a-11 thereunder. On May 19, 2022, Mimecast was acquired and taken private.

Facts

6. At all relevant times, Mimecast was a provider of cloud security and risk management services for email and corporate information. As a result, Mimecast's information technology network and resources regularly stored and transmitted its own data and code. During the relevant period, Mimecast disclosed in its periodic public filings with the Commission that it had approximately 40,000 customers.

7. In January 2021, Mimecast learned that it had been compromised by the same threat actor that was responsible for the SolarWinds Orion software compromise.

8. An investigation by Mimecast revealed that the threat actor exfiltrated a Mimecast-issued authentication certificate used to connect Mimecast to Microsoft and compromised five customers' cloud platforms using the stolen certificate. The threat actor also accessed internal email, most of the authentication and exgestion data export code used in Mimecast software, an encrypted database containing credentials for approximately 31,000 customers, and server and configuration information for approximately 17,000 customers. The investigation found no evidence that the threat actor had accessed relevant decryption keys or had accessed customer email or archive data.

9. In early 2021, Mimecast publicly disclosed certain aspects of the Compromise through a number of Forms 8-K filed with the Commission. However, Mimecast negligently omitted a number of material aspects of the Compromise, including information regarding the large number of impacted customers and the percentage of code exfiltrated by the threat actor.

10. On January 12, 2021, Mimecast filed a Form 8-K with the Commission disclosing that it had recently been informed that "a Mimecast-issued certificate provided to certain customers to authenticate Mimecast Sync and Recover, Continuity Monitor and IEP products to Microsoft 365 Exchange Web Services has been compromised by a sophisticated threat actor."

11. The January 12, 2021 Form 8-K further disclosed that approximately ten percent of its users used the connection impacted by the stolen certificate, and that “a low single digit number of [its] customers’ M365 tenants were targeted.”

12. On January 26, 2021, Mimecast filed an additional Form 8-K providing an update regarding its investigation into the Compromise: “Our investigation has now confirmed that this incident is related to the SolarWinds Orion software compromise and was perpetrated by the same sophisticated threat actor. Our investigation also showed that the threat actor accessed, and potentially exfiltrated[5], certain encrypted service account credentials created by customers hosted in the United States and the United Kingdom. These credentials establish connections from Mimecast tenants to on-premise and cloud services, which include LDAP, Azure Active Directory, Exchange Web Services, POP3 journaling, and SMTP-authenticated delivery routes.”

13. On March 16, 2021, Mimecast filed a Form 8-K with the Commission disclosing the results of its investigation into the Compromise. The Form 8-K stated, in part: “the evidence showed that this certificate was used to target only the small number of customers . . . ”

14. Through these public filings, however, Mimecast failed to report that the threat actor had accessed a database containing encrypted credentials for approximately 31,000 customers and server and configuration information for approximately 17,000 customers. The disclosures further omitted the material information that the threat actor gained access to tens of thousands of customers’ credentials as part of the Compromise, representing the majority of its customers.

15. In addition, the March 16, 2021 Form 8-K disclosed: “The investigation revealed that the threat actor accessed and downloaded a limited number of our source code repositories, as the threat actor is reported to have done with other victims of the SolarWinds Orion supply chain attack. We believe that the source code downloaded by the threat actor was incomplete and would be insufficient to build and run any aspect of the Mimecast service. We found no evidence that the threat actor made any modifications to our source code nor do we believe that there was any impact on our products. We will continue to analyze and monitor our source code to protect against potential misuse.”

16. In discussing the accessing of Mimecast’s source code, Mimecast stated that the source code downloaded was “incomplete and would be insufficient to build and run any aspect of the Mimecast service” and that it involved a “limited number” of code repositories. But Mimecast in the March 16, 2021 Form 8-K omitted that the threat actor had exfiltrated 58% of its exgestion source code, 50% of its M365 authentication source code, and 76% of its M365 interoperability source code, representing the majority of the source code for those three areas. Although the exfiltrated code represented a small portion of Mimecast’s complete product code, the functions it served were important to the security of Mimecast’s overall service offering, and therefore, its exposure to a reportedly nation-state-supported threat actor would be material to Mimecast’s investors.

[5] The term “exfiltration” refers to the unauthorized transfer of data from an information system.

17. In these public filings, Mimecast negligently created a materially misleading picture of the Compromise, providing quantification regarding certain aspects of the Compromise but not disclosing additional material information on the scope and impact of the incident. 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. Yet, Mimecast's disclosures omitted material information known to Mimecast at the time of the filing, including that the threat actor accessed and exfiltrated a large percentage of its source code related to exgestion, M365 authentication, and M365 interoperability code.

18. Throughout the periods discussed above, including following the filing of the January and March 2021 Forms 8-K, Mimecast offered and sold securities to its employees.

Violations

19. As a result of the conduct described above, Mimecast 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."

20. As a result of the conduct described above, Mimecast 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."[6]

21. As a result of the conduct described above, Mimecast violated Section 13(a) of the Exchange Act and Rule 13a-11 thereunder, which require issuers of a security registered pursuant to Section 12 of the Exchange Act to file with the Commission current reports on Form 8-K in conformity with the Commission's rules and regulations. Mimecast also violated Rule 12b-20 of the Exchange Act, which, among other things, requires such issuers to include in reports filed with the Commission any material information necessary to make the required statements in the filing not misleading.

Mimecast's Cooperation

22. In determining to accept the Offer, the Commission considered remedial acts undertaken by Mimecast and Mimecast's extensive cooperation afforded the Commission staff, which Mimecast provided consistently and throughout the entirety of the investigation. This cooperation included giving the staff detailed explanations, analysis, and summaries of multiple specific factual issues and promptly following up on the staff's requests for additional documents

[6] Violations of Sections 17(a)(2) and 17(a)(3) of the Securities Act do not require scienter and may rest on a finding of negligence. *See Aaron v. SEC*, 446 U.S. 680, 685, 701-02 (1980).

and information. In addition, Mimecast conducted an internal investigation, shared its findings with the staff on its own initiative, and took certain steps to enhance its cybersecurity controls. Mimecast's cooperation significantly contributed to the efficiency of the staff's investigation.

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-11 thereunder.

B. Respondent shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of $990,000 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;

(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 Mimecast Limited 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, Deputy Unit Chief, Crypto Assets and Cyber Unit, Division of Enforcement, Securities and Exchange Commission, 100 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 $990,000 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