UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 11321 / October 22, 2024

SECURITIES EXCHANGE ACT OF 1934
Release No. 101399 / October 22, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-22270

In the Matter of **Check Point Software Technologies Ltd.,** **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 Check Point Software Technologies Ltd. ("Check Point" 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 Check Point, a provider of products and services for information technology ("IT") security, negligently made to investors about Check Point's cybersecurity risks. In December 2020, Check Point identified two servers on its network that had versions of SolarWinds Orion software, which had been infected with malicious code by a persistent and reportedly nation-state-supported threat actor[2] that allowed for unauthorized activity on affected computers and their networks ("SolarWinds Compromise"). Shortly thereafter, a third-party vendor also notified Check Point of potential unauthorized activity in the Check Point environment. After an internal investigation, which commenced shortly after the discovery of the unauthorized activity, Check Point determined that the malicious activity in the Check Point environment related to the SolarWinds Compromise occurred at specific points during a four-month period from July through October 2020, and that this activity included communications with the threat actor's command-and-control server and execution of unauthorized software, including data compression software often used before data exfiltration.[3] Through the internal investigation, Check Point further determined that two Check Point corporate accounts had been compromised. The investigation also revealed instances of the threat actors attempting to move laterally in the Check Point environment.

2. On April 2, 2021 and April 14, 2022, Check Point filed reports on Forms 20-F with the Commission, which included materially misleading statements regarding Check Point's cybersecurity risks. Specifically in these public filings, Check Point included cybersecurity risk factor disclosures that were virtually unchanged from the same disclosures in prior Check Point public filings, even though Check Point had since identified, through its investigation, the foregoing, long-term cybersecurity compromise. In these disclosures, Check Point had described and continued to describe the existence of intrusions in generic terms only and omitted new and material cybersecurity risks arising out of the SolarWinds Compromise. Check Point failed to tailor them to Check Point's particular risks and incidents.

3. Based on the foregoing conduct, and the conduct described below, Check Point 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-1 thereunder.

Respondent

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

4. Check Point is an Israeli corporation with headquarters in Tel Aviv, Israel. During the relevant period, its stock has traded on NASDAQ under the ticker symbol CHKP, and its common stock was registered under Section 12(b) of the Exchange Act. Check Point is required to file with the Commission annual reports on Form 20-F pursuant to Section 13 of the Exchange Act and Rule 13a-1 thereunder.

Facts

5. At all relevant times, 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. As a result, Check Point's IT network and resources regularly stored and transmitted their own data and code.

6. On December 14, 2020, after learning about the SolarWinds Compromise from publicly available sources, Check Point identified instances of infected SolarWinds installations on two Check Point servers.

7. On December 15, 2020, a third-party vendor notified Check Point of potential unauthorized activity in the Check Point environment related to the SolarWinds Compromise.

8. Throughout December 2020, Check Point 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 Investigation, 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." The event impacted thousands of SolarWinds' customers.

9. Check Point began an internal investigation in December 2020. Check Point's investigation into the impact of the SolarWinds Compromise revealed 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, including a compression utility commonly used by hackers before exfiltrating data; compromise of two corporate accounts; and network reconnaissance and attempted lateral movement.

10. At the time of Check Point's investigation, which began in December 2020, many of the logs of network and internet activity were limited to September through December 2020, and therefore did not include logs of all unauthorized activity that could have occurred before that timeframe, which prevented it from identifying the full scope of the compromise. Check Point's investigation of the SolarWinds Compromise for those four months did not identify evidence of any additional activity including evidence that any customer data, code, or other sensitive information was accessed.

11. As a provider of enterprise IT services, Check Point's ability to protect its data and code is critically important to its reputation and ability to attract customers. Given its role and business, Check Point's information and data also were of great interest to state-sponsored cyber threat actors, such as the threat actor likely behind the SolarWinds Compromise.

12. Check Point's cybersecurity risk profile changed materially as a result of the SolarWinds Compromise-related activity in its network because of the following factors: (1) a likely nation-state-supported threat actor activated the SolarWinds vulnerability and used it to enter Check Point's environment; and (2) the threat actor persisted in the network unmonitored for several months and took steps, including deployment and removal of unauthorized software and attempting to move laterally, in Check Point's environment.

13. On April 2, 2021 and April 14, 2022, Check Point filed its annual reports on Forms 20-F with the Commission. In both reports, Check Point framed its cybersecurity risks generically. Specifically, Check Point failed to update its risk disclosures in light of the threat actor's infiltration of the Check Point network. The relevant cyber risk disclosures in Check Point's 2021 and 2022 Forms 20-F were identical to Check Point's disclosure on its April 2, 2020 Form 20-F, and therefore did not reflect the material change in its cyber security risks resulting from the SolarWinds Compromise.

14. In those Form 20-F disclosures, Check Point stated: "We regularly face attempts by others to gain unauthorized access through the Internet or to introduce malicious software to our information technology (IT) systems" and that "Additionally, malicious hackers may attempt to gain unauthorized access . . . " The disclosures further stated: "From time to time we encounter intrusions or attempts at gaining unauthorized access to our products and network. To date, none have resulted in any material adverse impact to our business or operations."

15. Check Point's disclosures in its 2021 Form 20-F and 2022 Form 20-F were rendered materially misleading by the omission of how the company's cybersecurity risk had increased due to the SolarWinds Compromise-related activity in its network, and Check Point's inability to fully assess the scope of activity prior to September 2020, because "there is a substantial likelihood that a reasonable shareholder would consider [this information] important" when evaluating Check Point's statements about intrusions and their impact on the company. *Basic, Inc. v. Levinson*, 485 U.S. 224, 299 (1988).

16. In addition to being inaccurate, 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. Commission Statement and Guidance on Public Company Cybersecurity Disclosure, Release Nos. 33-10459 at 13, 34-82746 (Feb. 21, 2018) *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf (emphasis added).[4] Specifically, its

[4] In addition to the Commission's 2018 cybersecurity guidance, the Commission has previously instructed issuers to provide tailored and non-generic risk disclosures in contexts other than cybersecurity. *See* Business and Financial Disclosure Required by Regulation S-K, Release No. 33-10064 (Apr. 13, 2016);

statements that Check Point "encounter[s] intrusions or attempts at gaining unauthorized access," were generic in the sense that they likely apply to every issuer of publicly-traded securities that uses information technology in its business. It was also generic and not tailored to Check Point's "particular … risks and incidents" because the relevant disclosures were identical to the 2020 cybersecurity risk factor disclosure, and therefore failed to reflect the changes in Check Point's cybersecurity risks between 2020 and 2021, about which Check Point knew about before April 2021 as a result of its investigation of the SolarWinds Compromise-related activity. Disclosing cybersecurity risks in only a generic way created a materially misleading impression of the cybersecurity risks that had arisen from the unmonitored presence of a likely nation-state-supported threat actor in Check Point's network, into which activity Check Point had limited visibility for the time period before September 2020. In combination with the facts that 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, these omissions were material. During this period, Check Point did not publicly make any statements or disclosures that corrected these misleading disclosures. 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."

17. Throughout the periods discussed above, including following the filing of the April 2, 2021 and April 14, 2022 Forms 20-F, Check Point offered and sold securities to its employees.

Violations

18. As a result of the conduct described above, Check Point 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."

19. As a result of the conduct described above, Check Point 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."[5]

20. As a result of the conduct described above, Check Point violated Section 13(a) of the 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. Check Point also violated Rule 12b-20 of the Exchange Act, which, among other things, requires such issuers to include in reports filed

---

Plain English Disclosure, Release No. 33-7497 (Jan. 28, 1998); and Updated Staff Legal Bulletin No. 7: Plain English Disclosure (Jun. 7, 1999) *available at* https://www.sec.gov/interps/legal/cfslb7a.htm.

[5] 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).

with the Commission any material information necessary to make the required statements in the filing not misleading.

Check Point's Cooperation

21. In determining to accept the Offer, the Commission considered remedial acts undertaken by Check Point and Check Point's significant cooperation afforded the Commission staff, which Check Point 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 and information. In addition, Check Point conducted an internal investigation, shared its findings with the staff on its own initiative, and took certain steps to enhance its cybersecurity controls. Check Point's cooperation meaningfully 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 and13a-1 thereunder.

B. Respondent shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of $995,000 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 Check Point Software Technologies Ltd. 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 $995,000 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