UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 10963 / August 16, 2021

SECURITIES EXCHANGE ACT OF 1934
Release No. 92676 / August 16, 2021

ADMINISTRATIVE PROCEEDING
File No. 3-20462

In the Matter of

Pearson plc,

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 Pearson plc ("Pearson" 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 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 that:

Summary

Pearson, a multinational educational publishing and services company, made material misstatements and omissions regarding a 2018 cyber intrusion that affected several million rows of student data across 13,000 school, district, and university AIMSweb 1.0 customer accounts in the United States. In its July 26, 2019 report furnished to the Commission, Pearson's risk factor disclosure implied that Pearson faced the hypothetical risk that a "data privacy incident" "could result in a major data privacy or confidentiality breach" but did not disclose that Pearson had in fact already experienced such a data breach. On July 31, 2019, approximately two weeks after Pearson sent a breach notification to affected customers, in response to an inquiry by a national media outlet, Pearson issued a previously-prepared media statement that also made misstatements about the nature of the breach and the number of rows and type of data involved.

Based on the foregoing conduct, and the conduct described herein below, Pearson 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, 13a-15(a), and 13a-16 thereunder.

Respondent

1. Pearson is a publicly traded United Kingdom corporation with headquarters in London, United Kingdom. Pearson's ordinary shares trade on the London Stock Exchange in the United Kingdom under the ticker symbol PSON. Since 2000, Pearson's American Depository Receipts ("ADRs"), each representing one ordinary share, have been listed on the New York Stock Exchange ("NYSE") under the ticker symbol PSO. In connection with the listing of the ADRs on the NYSE, Pearson's ordinary shares are registered under Section 12(b) of the Exchange Act. Pearson files with the Commission annual reports on Form 20-F and also furnishes periodic reports on Form 6-K pursuant to Section 13(a) of the Exchange Act and related rules thereunder applicable to foreign private issuers.

Facts

2. At all relevant times, Pearson was an educational publishing and services company delivering, among other things, academic performance assessment services to school districts in the United States. One of the services Pearson, through its subsidiary(ies), offered to its school district customers was AIMSweb 1.0, a web-based software for entering and tracking students' academic performance. Each customer account also had school administrator accounts that allowed district personnel to log into AIMSweb 1.0 in order to update and view performance data, as well as run reports on it. As a result, AIMSweb 1.0 data also included names, titles, and work addresses of school personnel and usernames and hashed passwords the school personnel used to access AIMSweb 1.0. Throughout 2018 and most of 2019, Pearson had two versions of AIMSweb available to its customers: AIMSweb 1.0 and AIMSweb Plus. The AIMSweb 1.0 product was set

to be retired when the intrusion occurred and was taken offline in July, 2019 as previously scheduled.

3. On March 21, 2019, Pearson learned that millions of rows of data stored on the AIMSweb 1.0 server had been accessed and downloaded by a sophisticated threat actor using an unpatched vulnerability on this server. The vulnerability had been publicized by the software manufacturer as critical in September 2018 because it allowed an attacker remotely to execute arbitrary code on vulnerable servers. Although the patch for this vulnerability was available and Pearson received notice of the patch in September 2018, Pearson did not implement the patch until March 2019, after it learned of the attack.

4. Later on March 21, 2019, Pearson was provided with a copy of the stolen data. Subsequent analysis of the data showed that all the school district personnel usernames and hashed passwords for AIMSweb 1.0 had been exfiltrated by a sophisticated threat actor. The school district personnel passwords were scrambled using an algorithm that had become outdated for protecting passwords. In addition, 11.5 million rows of student data had been exfiltrated.[1] The exfiltrated student data included only names and approximately half contained the students' dates of birth and approximately 290,000 contained the students' email addresses.

5. In March 2019, Pearson created an incident management response team and retained a third-party consultant to investigate the breach. In the course of this investigation, Pearson decided that it was not necessary to issue a public statement regarding the incident. On May 7, 2019, Pearson prepared a reactive media statement, which it planned to issue in the event of a significant media inquiry about the incident.

6. On July 19, 2019, after completion of its review of the incident, Pearson mailed a breach notice to all of its customer accounts whose student and school officials' credential data was exfiltrated from the AIMSweb 1.0 platform (approximately 13,000 accounts). The recipients included not only the then-current users of AIMSweb 1.0, but also the former users of AIMSweb 1.0 who had switched to the newer version of the platform. Because the notices did not inform school administrators that their usernames and hashed passwords were exfiltrated, the impacted accounts continued to be at risk after July 19, 2019. To the extent AIMSweb 1.0 users who switched to newer version of the platform recycled their credentials in the new version of the system, these accounts in the new system also continued to be at risk for a period of time after the July 19, 2019 notices.

7. On July 25, 2019, Pearson's management met to discuss the incident and again decided that it was not necessary to issue a public statement regarding it. On July 26, 2019, Pearson furnished on Form 6-K its report of interim results for the six months from January 1, 2019 through to June 30, 2019. In the "Principal risks and uncertainties" section of that report, Pearson stated that a "[r]isk of a data privacy incident or other failure to comply with data privacy regulations and standards and/or a weakness in information security, including a failure to prevent

[1] There were 11.5 million rows of student data but that number included duplication of student data when, for example, students moved from one school district to another, or when school administrators otherwise created duplicative records for the same students (for example, for each year the student was in the district or related to various activities the student participated in).

Also available as part of the eCourse
2021 Government Enforcement eConference

First appeared as part of the conference materials for the
7th Annual Government Enforcement Institute session
"Opening Keynote Presentation: Words Matter"