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).

or detect a malicious attack on our systems, could result in a major data privacy or confidentiality breach causing damage to the customer experience and our reputational damage, a breach of regulations and financial loss." This statement, which remained unchanged from prior Forms 6-K, implied that no "major data privacy or confidentiality breach" had occurred when Pearson knew months earlier about the AIMSweb 1.0 breach. Pearson failed to consider how certain information about that breach should have informed this risk disclosure.

8. On July 31, 2019, a reporter from a national media outlet contacted Pearson regarding an impending article describing Pearson's data breach. Pearson gave the reporter the media statement it had drafted on May 7, 2019 with the sole change that the statement specifically referred to AIMSweb 1.0.

9. Later that evening on July 31, 2019, Pearson posted the media statement on its website. The media statement was misleading for the following reasons:

a. Although Pearson had known for months that the threat actor removed several million rows of data from the AIMSweb 1.0 server, rather than just having obtained access to view the data, the statement referred to the incident as "unauthorized access" and "expos[ure of] data."

b. The media statement also misstated that the impacted "data was isolated to first name, last name, and in some instances may include date of birth and/or email address," even though usernames and hashed passwords of school personnel were also exfiltrated.

c. The media statement characterized the exfiltration of dates of birth and email addresses as hypothetical: "*may* include date of birth and/or email address" (emphasis added). In fact, Pearson knew that approximately half of the exfiltrated data contained dates of birth and approximately 290,000 contained email addresses.

d. The media statement omitted that millions of rows of student data were involved in the breach.

e. The media statement also included the statement "Protecting our customers' information is of critical importance to us. We have strict data protections in place and have reviewed this incident, found and fixed the vulnerability." Pearson also stated that "While we have no evidence that this information has been misused, we have notified the affected customers as a precaution." The sophisticated threat actor obtained access to the AIMSweb 1.0 server through a critical vulnerability, which Pearson failed to patch for six months after it was notified; Pearson was using a hashing algorithm for password storage that had become outdated.

10. The next trading day following Pearson's media statement, Pearson's stock price on the NYSE declined by 3.3% on August 1, 2019.

11. The breach at issue was material because Pearson's business, including but not limited to AIMSweb 1.0, involved collection and storage of large quantities of private data on school-age children around the world. As Pearson acknowledged in its risk disclosures, Pearson "holds large volumes of personally identifiable information," and its reputation and ability to attract and retain revenue depended in part on its ability "to adequately protect personally identifiable information." This breach involved a compromise of a server holding a large quantity of data Pearson was responsible for protecting and exfiltration of a significant number of student names, dates of birth, and email addresses, and school administrator login credentials. It also involved lapses in Pearson's protection of that data.

12. Throughout the periods discussed above, including following the furnishing of the above-referenced Form 6-K on July 26, 2019 and the posting of the media statement on July 31, 2019, Pearson was engaged in an ongoing offering of its ordinary shares under the company's employee and management incentive plans to Pearson employees.

13. Pearson's processes and procedures around the drafting of its July 26, 2019 Form 6-K Risk Factor disclosures and its July 31, 2019 media statement failed to inform relevant personnel of certain information about the circumstances surrounding the breach. Although protecting student and user data is critical to Pearson's business, and Pearson had identified the potential for improper access to such data as a significant risk, it failed in this way to maintain disclosure controls and procedures designed to analyze or assess such incidents for potential disclosure in the company's filings.

Pearson's Cooperation

14. In determining to accept the Offer, the Commission considered Respondent's cooperation afforded the Commission staff.

Violations

15. As a result of the conduct described above, Pearson violated Sections 17(a)(2) and 17(a)(3) of the Securities Act [15 U.S.C. §§ 77q(a)(2) and (3)], which make it unlawful for any person in the offer or sale of any securities by the use of any means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly, to obtain 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; or to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser.[2]

16. As a result of the conduct described above, Pearson violated Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 12b-20 and 13a-16 thereunder [17 C.F.R. §§ 240.12b-20, 240.13a-16], which require every foreign issuer of a security registered pursuant to

[2] A violation of these provisions does not require scienter and may rest on a finding of negligence. *See Aaron v. SEC*, 446 U.S. 680, 685, 701-02 (1980).

Section 12 of the Exchange Act to furnish the Commission with periodic reports containing information that is accurate and not misleading.

17. As a result of the conduct described above, Pearson violated Rule 13a-15(a) of the Exchange Act [17 C.F.R. § 240.13a-15(a)], which requires every issuer to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or furnishes pursuant to the Exchange Act is recorded, processed, summarized, and reported, within the time period specified in the Commission's rules and forms.

IV.

In view of the foregoing, the Commission deems it appropriate to impose the sanctions agreed to in Respondent Pearson'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, 13a-15(a), and 13a-16 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;

(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 Pearson plc 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 A. Kristina Littman, Cyber Unit

Chief, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 20549.

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.

By the Commission.

Vanessa A. Countryman
Secretary