SULLIVAN & CROMWELL LLP

S&C memo

August 18, 2021

SEC Charges Issuer with Misleading Investors About Cybersecurity Incident and for Inadequate Disclosure Controls

Action Underscores SEC's Heightened Focus on the Timely and Effective Remediation and Disclosure of Cybersecurity Incidents

SUMMARY

On August 16, 2021, the SEC charged Pearson plc with misleading investors and failing to maintain adequate disclosure controls and procedures in connection with a cybersecurity incident. According to the SEC's order, Pearson learned in March 2019 about an intrusion involving the exfiltration of millions of rows of student data, including names and some birthdates and email addresses, as well as usernames and hashed passwords for school personnel. In July 2019, a periodic filing characterized data privacy incidents as an ongoing risk factor but failed to disclose that such an incident—and one characterized by the Order as "material"—had actually occurred. The SEC also found Pearson's later media statement misleading in several respects. Additionally, the SEC found that Pearson failed to maintain disclosure controls and procedures sufficient to appropriately assess cybersecurity incidents for potential disclosure. The Order, which reflected settled charges, imposed a $1 million penalty. The enforcement action underscores the recent, increased focus by the SEC on the timely and effective remediation and disclosure of cybersecurity incidents.

BACKGROUND

Pearson plc ("Pearson") is an educational publisher and services provider headquartered in the United Kingdom.[1] During the relevant time period, Pearson's offerings included AIMSweb 1.0, a web-based software program for tracking students' academic performance. Using AIMSweb 1.0, school district personnel could access, update, and run reports on student performance data.

According to the cease-and-desist order (the "Order"), Pearson learned on March 21, 2019 that a "sophisticated threat actor" had both accessed and downloaded millions of rows of data from the AIMSweb 1.0 server.[2] The SEC found that "[s]ubsequent analysis . . . showed that all the school district personnel usernames and hashed passwords for AIMSweb 1.0 had been exfiltrated," as well as "11.5 million rows of student data" consisting of student names and, for some of the data, birthdates and email addresses.[3] The Order stated that Pearson had failed to patch the vulnerability that was eventually exploited by the threat actor, despite receiving notice about the vulnerability and an available patch from the software manufacturer six months prior.

According to the Order, Pearson "created an incident management response team and retained a third-party consultant to investigate the breach" but ultimately decided against issuing a public statement.[4] On July 19, 2020, after completing an incident review, Pearson notified the approximately 13,000 customer accounts impacted by the breach. However, some accounts that had switched to a newer version of the software but used the same credentials allegedly still remained vulnerable because the notifications failed to inform school district personnel that their usernames and hashed passwords had been compromised.

On July 26, 2019, Pearson filed a Form 6-K for the first half of 2019. In the form's section on risk factors, Pearson listed the risk of "a major data privacy or confidentiality breach" and the negative consequences that could ensue.[5] The SEC found that the phrasing of the statement—"unchanged from prior Forms 6-K"—suggested that no such incident had actually occurred.[6] According to the Order, "Pearson failed to consider how certain information about [the AIMSweb 1.0 breach] should have informed this risk disclosure."[7]

On July 31, 2019, Pearson issued a media statement after a reporter contacted the company about the incident. According to the Order, on the next trading day following the media statement (August 1, 2019), the company's stock price on the NYSE fell by 3.3%. The SEC found the media statement misleading because it (i) characterized the incident as involving "unauthorized access" and "expos[ure of] data," when Pearson knew that the threat actor actually removed data from the server; (ii) stated that impacted data "may" include birthdates/email addresses, when Pearson knew that some of the exfiltrated data did, in fact, include such information; (iii) stated that impacted data was limited to names (and "may" include birthdates/email addresses), when Pearson knew that usernames and hashed passwords were also exfiltrated; (iv) stated that protecting customer information was of "critical importance" to Pearson and Pearson had "strict data protections in place," when "Pearson failed to patch for six months after it was notified" and used an outdated password hashing algorithm; and (v) omitted that the breach involved "millions of rows of student data."[8]

The Order also found that the breach was "material."[9] Noting that Pearson's business involved "large quantities of private data on school-age children," the SEC found that the company's "reputation and ability

to attract and retain revenue" relied in part on the company's ability to safeguard large amounts of personally identifiable information.[10] The Order also noted that the incident "involved a compromise of a server holding a large quantity of data Pearson was responsible for protecting," "exfiltration of a significant number of student names, dates of birth, and email addresses, and school administrator login credentials," and "lapses in Pearson's protection of that data."[11]

Finally, with respect to disclosure controls and procedures, the SEC stated that the processes surrounding the drafting of the Form 6-K and the media statement "failed to inform relevant personnel of certain information about the circumstances surrounding the breach."[12] The Order did not identify the relevant personnel or specify the information about which they were not informed.

On the basis of the allegedly misleading disclosures, the Order charged violations of Sections 17(a)(2) and 17(a)(3) of the Securities Act and violations of Section 13(a) of the Exchange Act and Rules 12b-20 and 13a-16 thereunder.[13] The Order also charged a violation of Rule 13a-15(a) of the Exchange Act, which requires covered issuers "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" by the SEC.[14] Without admitting or denying the SEC's findings, Pearson submitted an Offer of Settlement and agreed to pay a civil money penalty of $1 million and to cease and desist any future violations.[15]

IMPLICATIONS

This action is the latest in which the SEC has found a violation of the securities laws where a company presented cybersecurity or other risk in its periodic filings as merely hypothetical when the risk had in fact materialized. For example, in 2019, in connection with the Cambridge Analytica scandal, the SEC fined Facebook $100 million for "present[ing] the risk of misuse of user data as merely hypothetical when Facebook knew that a third-party developer had actually misused Facebook user data."[16] In this action, the SEC similarly focused on the company's public statement that certain types of data "may" have been compromised as merely hypothetical when the company knew that such data had, in fact, been compromised.[17] In an environment of heightened cybersecurity risk for companies around the world, the action underscores the SEC's continuing focus on ensuring that companies' statements about cybersecurity risks and incidents provide timely and accurate information about the nature of the company's experience. Companies should ensure that risk factors and other disclosures and public statements are adequately and timely reviewed on a regular basis, including considering updating risk factors in periodic filings during the year.

The action also reflects the SEC's recent, heightened emphasis on disclosure controls and procedures in cybersecurity, particularly those related to critical software vulnerabilities and timely remediation of significant cybersecurity incidents. In June 2021, the SEC brought another action based on disclosure

controls and procedures against First American Financial Corporation alleging, as here, that the company failed to timely remediate a critical software vulnerability that exposed millions of consumer records and lacked disclosure controls and procedures sufficient to ensure that accurate information concerning the incident was escalated to those in charge of the company's disclosures.[18] These actions also coincide with the SEC's widely reported, voluntary request to many companies seeking information about companies' experience with the compromise of SolarWinds software, which significantly impacted many federal government agencies and some private sector companies. As we wrote in our client memorandum addressing the *First American* action, and this action further confirms, the SEC appears particularly focused on timely escalation and remediation of cybersecurity risks and incidents at a time when companies across industries in the United States are experiencing an onslaught of cyberattacks, from systemic supply-chain and vulnerability compromises to ransomware attacks and cyber-extortion schemes.

Finally, the SEC's characterization of the company's underlying cybersecurity incident as "material" is noteworthy. The core of the SEC's rationale for that characterization—that the company handles a large volume of personally identifiable information and thus its reputation and business depend in part on maintaining the security of that information—may apply to many companies across industries. Further, while the breach was significant, the categories of data affected in the incident, including dates of birth, email addresses, usernames and hashed passwords, were no more sensitive than many other types of personally identifiable information regularly impacted in data breaches, including Social Security, passport, and credit card numbers and other information. It remains to be seen whether the case signals that the SEC will implement a broader interpretation of materiality in the cybersecurity breach context. Companies should consider this uncertainty in assessing their disclosures regarding cybersecurity incidents.

* * *

ENDNOTES

1 *In the Matter of Pearson plc*, Securities Act Release No. 10963, Exchange Act Release No. 92676 (Aug. 16, 2021).

2 *Id.* at ¶ 3.

3 *Id.* at ¶ 4.

4 *Id.* at ¶ 5.

5 *Id.* at ¶ 7.

6 *Id.*

7 *Id.*

8 *Id.* at ¶ 9.

9 *Id.* at ¶ 11.

10 *Id.*

11 *Id.*

12 *Id.* at ¶ 13.

13 *Id.* at ¶¶ 15-16.

14 *Id.* at ¶ 17.

15 *Id.* at p. 6.

16 Press Release, *Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data*, U.S. Secs. & Exchange Comm'n (July 24, 2019), https://www.sec.gov/news/press-release/2019-140. *See also* our previous Client Memorandum, "FTC Settlement with Facebook Over Privacy Policies Imposes Unprecedented Penalties and Restrictions," dated July 26, 2019, available at https://www.sullcrom.com/ftc-settlement-with-facebook-over-privacy-policies-imposes-unprecedented-penalties-and-restrictions.

17 Similar claims by plaintiffs have also been allowed in private securities litigation. *See, e.g.*, *In re Alphabet, Inc. Sec. Litig.*, 1 F.4th 687, 703-04 (9th Cir. 2021).

18 Press Release, *SEC Charges Issuer With Cybersecurity Disclosure Controls Failures*, U.S. Secs. & Exchange Comm'n (June 15, 2021), https://www.sec.gov/news/press-release/2021-102.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.