HINSHAW

Alerts

SEC Lessons Learned: Public Companies Must Accurately Disclose Material Cyber Breaches to Investors

August 24, 2021
Hinshaw Privacy & Cyber Bytes

On August 16, 2021, the Securities and Exchange Commission (SEC) announced a $1 million settlement with Pearson plc (Pearson) in connection with a 2018 "cyber intrusion" that resulted in the theft of millions of student records, along with the login credentials of 13,000 schools, district and university customer accounts. The settlement came after the SEC found that the UK-based multinational educational publishing and services company had knowingly made misleading statements and omissions to investors and others regarding the data breach. Although Pearson admits to no wrongdoing, it has committed to not making any misleading statements or omissions to investors in the future as part of the settlement.

The SEC Cease and Desist Order

The SEC's findings concerning Pearson's conduct can be found in its formal "Order Instituting Cease and Desist Proceedings, pursuant to Section 7A 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" (the Order). In the Order, the SEC asserted that in March of 2019, Pearson learned that a "sophisticated threat actor" had downloaded millions of rows of data using an unpatched vulnerability on Pearson's AIMSweb 1.0 software, which tracks students' academic performance. Although a patch for this vulnerability was known and available, Pearson did not implement it until after the breach occurred.

The SEC further found that Pearson made several misleading statements and omissions about the breach. For example, the breach notice to affected customer accounts failed to disclose that usernames and passwords had been compromised, thereby exposing the relevant accounts to continued risk. Pearson also issued a six-month lookback report to investors after the breach "that implied that 'no major data privacy or confidentiality breach' had occurred." Pearson only publicly acknowledged the breach after it was contacted by a national media outlet regarding a forthcoming article describing the incident. Even then, according to the Order, the public media statement misrepresented the extent of the breach; the protections Pearson had in place to avoid such an event; and omitted the fact that millions of rows of student data, usernames, and passwords were compromised. Finally, the SEC found that Pearson lacked

Attorneys

Samantha R. Millar

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

adequate "disclosure controls and procedures" to ensure that individuals responsible for making disclosure determinations were provided with material information about the circumstances surrounding the incident.

Based on these findings, the SEC concluded that Pearson violated Sections 17(a)(2) and 17(a)(3) of the Securities Act, which, in sum, makes it unlawful to make an untrue statement of material fact or omit a necessary material fact in connection with the offer or sale of securities. The SEC also found that Pearson's conduct violated various provisions of the Exchange Act.

The Takeaways

As the threat of data breaches and cyber intrusions continues to increase, public companies must ensure that timely and accurate information is provided to investors about cyber incidents. Recently, the SEC has brought several other cybersecurity disclosure cases resulting in significant settlements and fines, including a $35 million settlement in 2018 resolving allegations that Yahoo! Inc. failed to disclose to investors that it had been the victim of a data breach. The Commission has likewise warned that companies must have robust internal controls and procedures to detect cyber threats and adequately disclose material information regarding data breaches.