Simpson Thacher

Regulatory and Enforcement Alert

SEC Settles Charges With Pearson plc Relating to Disclosures Concerning Cyber Breach

August 17, 2021

Key Takeaways

- *The case reflects the SEC's continued focus on accurate disclosures and robust disclosure controls in connection with cyber incidents.*
- *Warning that an event (such as a cyber incident) "may" occur will not suffice when that event has already occurred.*
- *Sound disclosure controls require that those responsible for disclosure decisions have before them all of the relevant information.*

On August 16, 2021, the SEC announced that Pearson plc agreed to pay $1 million to settle administrative charges that it provided investors with inaccurate information regarding a 2018 cyberattack that resulted in the theft of millions of student records and failed to maintain adequate disclosure controls and procedures regarding such incidents. The charges signal that the SEC continues to focus on the need for public companies to provide accurate information about cyber-related events and data privacy.

Pearson, a U.K.-based educational publishing firm that provides services to schools and universities, suffered a data breach relating to millions of student accounts and records, along with the administrator login credentials of thousands of schools, districts and universities. According to the SEC's order, the company characterized the "[r]isk of a data privacy incident" as hypothetical in its 2019 Form 6-K (consistent with the company's prior Forms 6-K) when it knew that a data breach had occurred months earlier. The order states that upon learning of the breach, and in advance of issuing the Form 6-K, Pearson had created an incident management response team and had retained a third-party consultant to investigate the breach, but did not modify the language in its Form 6-K or otherwise issue a public statement regarding the incident.

The SEC found that Pearson only disclosed the breach after it was contacted by the media, and did so in a manner that understated both the nature and scope of the breach. Among other things, Pearson stated that the breach may have included dates of birth and email addresses of students when it knew that such data had in fact been stolen; failed to disclose that the breach involved millions of rows of student data; and omitted that data was removed from its server rather than just having been viewed. The order further found that Pearson stated that it had "strict

protections" in place and had "found and fixed the vulnerability" when the server had been accessed through a "critical vulnerability" and Pearson did not remedy the weaknesses for six months after learning of the breach.

Finally, the SEC order found that Pearson's disclosure controls were not reasonably designed to ensure that personnel with authority for disclosure decisions had all of the relevant information regarding the data breach.

Cases involving disclosures that depict risks, events, or conflicts of interest as something that "may" or "might" occur when in fact they are known to have occurred have long been a staple of the SEC's enforcement program—and they provide a straightforward basis for the type of negligence-based disclosure charges at issue here. The Pearson settlement is in keeping with this established principle, and reflects the SEC's continued focus—going back to the creation of the Cyber Unit in 2017, the Yahoo! disclosure settlement in 2018 and continuing more recently in June 2021 with the First American Financial Corporation disclosure controls settlement—on the adequacy of cyber disclosures and related controls.

For further information regarding this Alert, please contact any member of the **Government and Internal Investigations** Group or **Privacy and Cybersecurity** Practice below.

GOVERNMENT AND INTERNAL INVESTIGATIONS GROUP/PRIVACY AND CYBERSECURITY PRACTICE

Antonio Bavasso
+44-(0)20-7275-6122
antonio.bavasso@stblaw.com

Martin S. Bell
+1-212-455-2542
martin.bell@stblaw.com

Marc P. Berger
+1-212-455-2197
marc.berger@stblaw.com

Stephen P. Blake
+1-650-251-5153
sblake@stblaw.com

Brooke E. Cucinella
+1-212-455-3070
brooke.cucinella@stblaw.com

Paul C. Curnin
+1-212-455-2519
pcurnin@stblaw.com

Stephen M. Cutler
+1-212-455-2773
stephen.cutler@stblaw.com

Sarah L. Eichenberger
+1-212-455-3712
sarah.eichenberger@stblaw.com

Adam Goldberg
+852-2514-7552
adam.goldberg@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Meaghan A. Kelly
+1-202-636-5542
mkelly@stblaw.com

Jeffrey H. Knox
+1-202-636-5532
jeffrey.knox@stblaw.com

James G. Kreissman
+1-650-251-5080
jkreissman@stblaw.com

Noritaka Kumamoto
+81-3-5562-6219
nkumamoto@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Joshua A. Levine
+1-212-455-7694
jlevine@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

Cheryl J. Scarboro
+1-202-636-5529
cscarboro@stblaw.com

John Terzaken
+1-202-636-5858
john.terzaken@stblaw.com

Jonathan K. Youngwood
+1-212-455-3539
jyoungwood@stblaw.com

Anar Rathod Patel
+1-212-455-2206
apatel@stblaw.com

Rafael M. Loureiro
+55-11-3546-1026
rafael.loureiro@stblaw.com