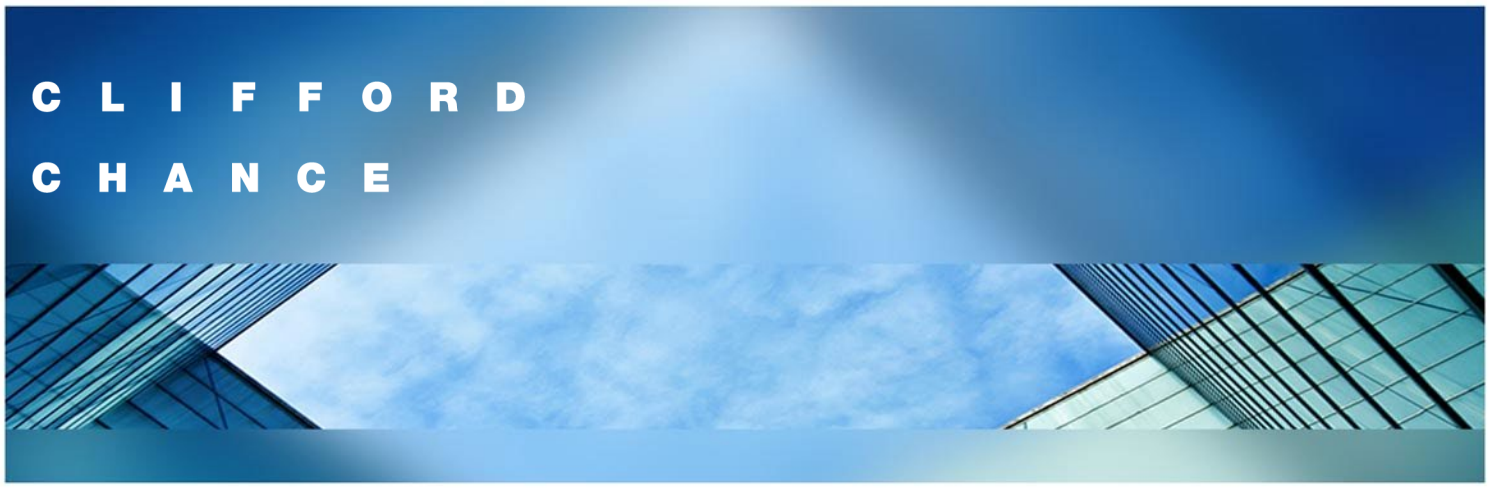

SEC CONTINUES FOCUS ON CYBERSECURITY WITH ENFORCEMENT ACTION AGAINST LONDON-BASED PUBLISHER

Continuing a recent trend of using disclosure rules to police cybersecurity, on August 16, 2021 the Securities and Exchange Commission ("SEC") announced a settlement with London-based publisher Pearson PLC for a 2018 cybersecurity breach that affected the personal data of millions of students. Pearson agreed to a USD 1,000,000 fine along with an order to cease and desist from committing or causing future violations. As with another cybersecurity-related enforcement action from June, the SEC charges against Pearson were not based on inadequate cybersecurity; rather, the SEC charged Pearson for making material misstatements and omissions regarding the incident. The penalty is a reminder that companies subject to SEC oversight (including foreign issuers) must take care to ensure their public disclosures are both accurate and precise.

Key issues

- The SEC fined a foreign issuer USD 1,000,000 for improper disclosures relating to a cybersecurity vulnerability that exposed personal data of millions of students.
- The SEC accused Pearson of making false and misleading statements in its public and required disclosures.
- The settlement underscores the importance of making sure disclosures are both accurate and precise. In particular, companies should avoid using hedging language like "may" or "could" unless they accurately describe the situation.

SEC DISCLOSURE RULES FOR FOREIGN ISSUERS

The Securities Act and Exchange Act have a number of provisions prohibiting issuers from making material misstatements and omissions to buyers of securities and the SEC. Section 17(a) of the Securities Act forbids the use of untrue statements or omissions of material facts in relation to the offer or sale of any securities in interstate commerce. Additionally, Rule 13a-15 of the Exchange Act requires issuers to maintain controls and procedures designed to ensure that required disclosures are timely reported pursuant to the Commission's rules. Section 13(a) of the Exchange Act requires foreign issuers to provide periodic reports to the SEC. Information in these reports must be accurate and not misleading. One of these reports is Form 6-K, which provides interim financial results and other required disclosures.

BACKGROUND: THE BREACH

According to the SEC order, the fine arose from events relating to a cybersecurity incident that Pearson discovered in March 2019. An attacker used an unpatched software vulnerability in Pearson's systems to access and download usernames and passwords for approximately 13,000 accounts. The attacker also stole 11.5 million rows of student data, about half of which contained the students' dates of birth; approximately 290,000 data rows also contained student email addresses.

After learning of the incident, Pearson put together an incident management response team and hired a third-party consultant to investigate the breach. This team decided no public statement was necessary; instead, Pearson prepared a reactive media statement, to be used if the event resulted in significant media attention.

In July, after completing its investigation of the breach, Pearson sent a breach notification letter to all compromised customer accounts. Pearson again decided, however, that no public statement was necessary. It only issued its reactive media statement a week later after a national media outlet contacted Pearson for comment on an upcoming story about the breach.

BACKGROUND: THE VIOLATIONS

According to the SEC order, Pearson made two sets of misstatements of material facts and material omissions.

First, in the Form 6-K it filed in July 2019, Pearson used the same cybersecurity disclosure it had used in previous Form 6-Ks while describing the risks it faces. This disclosure referred to cybersecurity incidents as a hypothetical risk that could lead to reputational damage and financial harm. The SEC said this statement implied that Pearson had not yet encountered any such incidents, even though it knew that it had recently experienced just such a breach.

Second, in its statement to the media, Pearson downplayed the incident, which the SEC alleged to be misleading. Pearson said that the data breach had led to unauthorized "access" and "exposure" of data, when in fact it knew that data had actually been removed from Pearson servers. Pearson also said the breach included names, dates of birth, and email addresses, even though it also knew that usernames and passwords were included in the preach. Additionally, while describing the type of data involved, it said that the breach "may" include dates of birth and email addresses, even though Pearson actually knew that at least some dates of birth and email addresses had actually been removed. The SEC also criticized Pearson for failing to include the number of potential data subjects affected in the breach. The SEC also took issue with Pearson's statement that it had "strict data protections in place," pointing out that Pearson had failed to patch the security vulnerability that led to the breach for six months after being notified of the risk, and had used outdated processes to protect user account passwords.

In addition to these improper disclosures, the SEC found that Pearson did not have proper controls and procedures in place to ensure that the senior executives responsible for making the disclosures were adequately informed of the circumstances surrounding the breach.

CONCLUSION

The SEC appears to be getting more involved in cybersecurity enforcement, with a special focus on ensuring that companies make proper disclosures regarding cybersecurity incidents. The Pearson action follows a similar one in June, when the SEC settled an enforcement action against a US title insurance company for inadequate disclosures related to a cybersecurity vulnerability in its system that exposed hundreds of millions of financial documents, many of which contained sensitive personal data such as social security numbers and financial information.[1] While the $1 million fine here against Pearson, like the $500,000 fine imposed in the Commission's earlier action, is not very substantial, the SEC's continued focus on the accuracy of cybersecurity-related disclosures signals that the SEC intends to maintain an active role in policing cybersecurity readiness, and transparency about that readiness.

The action also shows the danger in being too cautious in public and required disclosures. The SEC order specifically criticizes Pearson's use of hedging language like "could" and "may" in its statements, which the SEC says downplayed the severity of the breach such that they misled investors and the Commission. Disclosures and public statements must be both accurate and precise—companies should refrain from over-use of hedging qualifiers and ensure that any language recycled from previous disclosures continues to be appropriate.

Good cyber hygiene and risk management starts long before an incident occurs, and it is a global issue for multinational companies. Clifford Chance has published a number of reports and briefings to help companies protect themselves from attacks and vulnerabilities. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook. Also see our briefing here for more information on making required SEC disclosures.

[1] For more on the enforcement action against First American, see our briefing here.

CONTACTS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Managing Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Minji Reem
Associate

T +1 212 878 8027
E minji.reem
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.