BCLP. Client Intelligent

BCLPSecCorpGov.com

PRIVACY, VULNERABILITIES, AND BREACHES, OH MY

Aug 24, 2021

A recent SEC settlement shed light on data security and privacy concerns that public companies should keep in mind when drafting and filing periodic reports. The SEC settlement concerned a 2018 data breach at Pearson Plc that resulted in theft of user data, including sensitive personal data. The Pearson settlement resulted in entry of a Cease and Desist order prohibiting violations of the antifraud provisions of Securities Act Section 17(a), and Exchange Act Section 13(a)'s requirement that foreign issuers file accurate periodic reports and maintain controls to assure this. Pearson will pay a $1 million penalty as part of the resolution.

The charged conduct in Pearson's case focused on language from its SEC filings concerning protection of users' personal data, and the content of the company's disclosures after learning in March 2019 that this data had both been publicly exposed and stolen by bad actors. Pearson's failings represented the latest illustration of a favorite SEC principle underscored in countless enforcement actions, namely, that it is misleading to disclose a potential occurrence as a risk after it has already occurred. In the SEC's telling, Pearson's periodic filings continued to make the same standard disclosures of data privacy incident risks, including a statement that it was aware of no such events, even after Pearson learned that its user data had been exposed and stolen.

Beyond Pearson's failing to disclose the fact of the data theft, the SEC also charged it with making inaccurate media statements that minimized the nature of the incident. Pearson's disclosures referred only to the data's being exposed, rather than noting it was also stolen. And Pearson understated the data loss that occurred by inaccurately describing both the volume and type of personal data involved.

While not forming the factual basis for any charges, the SEC Order also stated that Pearson missed multiple opportunities to disclose the incident, waiting instead until after it had been contacted by the media. Further, the SEC pointed out that Pearson had for several months been aware of the vulnerability that caused the incident and the availability of a patch to fix it, but neglected to implement the patch until it learned of the data theft. Failure to disclose the incident, in particular, could easily be cited as the basis for a charge in a future action.

Overall, the Pearson case joins a recent Ninth Circuit decision involving a large technology company as reminders that issuer disclosures must use language that accurately portrays the certainty of

events, including disclosing as facts any events that have actually occurred (rather than obliquely referring to them as hypothetical "risks"). The *Pearson* and Ninth Circuit cases also demonstrated the SEC and court's reliance on the 2018 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, to determine the relevant materiality calculus for disclosing cybersecurity events ranging from vulnerabilities to breaches. Companies would do well to review these recent cases, and the SEC guidance, in advance of assessing disclosure of any such events.

RELATED CAPABILITIES

- Securities & Corporate Governance
