August 17, 2021

Latest SEC Enforcement Action Reinforces Critical Need to Maintain Effective Disclosure Controls Concerning Cybersecurity Breaches and Risks

In yet another important signal of the SEC's increasing focus on how public companies respond to, and issue disclosures concerning, significant cyber breaches, the Commission announced yesterday that it had entered into a settled administrative order with Pearson plc, finding violations of the negligence-based antifraud provisions of the Securities Act and imposing a $1 million civil penalty. Pearson neither admitted nor denied the Commission's findings.

The Order recites that a substantial volume of personal data concerning students and school administrators was stolen by a "sophisticated threat actor" from Pearson's academic performance assessment services that were provided to 13,000 school districts in the United States, and notes that while Pearson's periodic filings with the Commission contained risk-factor disclosure identifying that "malicious attack[s] on our systems" could result in a "'major data privacy or confidentiality breach,'" the Company re-issued that risk-disclosure language without disclosing that precisely such a major breach had occurred just a few months earlier. The SEC also found that Pearson's response to media inquiries concerning the breach was materially misleading, because its press statement downplayed the scale and seriousness of the breach and implied that certain types of personal data may have been obtained, when Pearson knew that such data had, in fact, been stolen.

In addition to finding that the Company's public statements were misleading, the Commission determined that Pearson failed to maintain disclosure controls and procedures properly designed to analyze and assess cybersecurity incidents such that management was able to make appropriate and accurate disclosure decisions.

Like the *First American Financial* proceeding we discussed in June, this most recent Commission action underscores that companies must take care to adequately inform decision-makers so that disclosure decisions concerning cybersecurity incidents are grounded in a full appreciation of all pertinent facts, and that, if they choose to make a public statement, it must be accurate and not misleadingly incomplete. Importantly also, yesterday's proceeding is a telling reminder that companies cannot reflexively re-issue standard risk-factor language without more if they have experienced a major undisclosed cyber breach involving

the actual theft of a substantial volume of sensitive data. As we have observed before, the understandable desire to reassure customers and data users in the midst of a cybersecurity crisis cannot be allowed to compromise fidelity to the disclosure requirements of the federal securities laws. Properly designed procedures and robust internal controls governing disclosure decision-making are the best bulwark against those risks, along with a crisis response team staffed by appropriate and well-advised experts.

John F. Savarese
Wayne M. Carlin
Sabastian V. Niles