Cooley

SEC Enforcement Targets Cybersecurity Disclosures Again

August 17, 2021

Securities and Exchange Commission Chairman Gary Gensler has pledged to bring a renewed focus to robust enforcement of the federal securities laws. As we observed in a recent blog post, under Chairman Gensler and Director Gurbir Grewal, the SEC's Division of Enforcement will be more aggressive in several arenas—including public company cybersecurity disclosures. Recent enforcement actions confirm that cybersecurity disclosures are a key area of focus for the new SEC leadership.

Despite a long-professed focus on public company cybersecurity disclosures, SEC enforcement actions in the space have been few and far between. Just in the past two months, however, the SEC filed two public company cybersecurity enforcement actions in quick succession. Neither action included allegations of intentional misconduct, or any charges against individuals. Instead, in both cases, the SEC brought charges based on the companies' alleged failure to maintain adequate disclosure controls and procedures, supplemented by negligence-based fraud charges in one case. By repeatedly pursuing non-scienter charges, the Enforcement Division has signaled that it will take a hard line against companies who have failed to fully and transparently disclose all material facts regarding cybersecurity incidents.

Strict enforcement for cybersecurity disclosures

First, on June 15, 2021, the SEC announced settled charges against title insurer First American Financial Corporation in connection with the company's June 2019 disclosures regarding a cybersecurity vulnerability. While First American claimed publicly that it had taken "immediate action" to address the vulnerability, the SEC found that at the time of the disclosures, the company's information security personnel had been aware of the vulnerability for months but did not inform the senior executives responsible for the company's public disclosures. First American agreed to an order charging it with failing to maintain adequate cybersecurity disclosure controls and requiring it to pay a $487,616 penalty.

Then, on August 16, 2021, the SEC announced settled negligence-based fraud and disclosure controls charges against Pearson plc, an educational services company headquartered in London. According to the SEC's order, in September 2018, Pearson was notified of a vulnerability on a server used by the company to store sensitive student data. The SEC found that although a patch for the vulnerability was made available to Pearson, the company failed to apply the patch. In March 2019, Pearson learned that the unpatched vulnerability had been exploited by a threat actor who accessed and downloaded 11.5 million rows of student data. Some of the stolen data included students' dates of birth and email addresses.

Pearson did not immediately disclose the intrusion. About three months after learning of the incident, however, the company submitted a filing to the SEC that contained a cybersecurity related risk factor. In the disclosure, the company stated that the hypothetical "isk of a data privacy incident or other failure to comply with data privacy regulations and standards and/or a weakness in information security, including a failure to prevent or detect a malicious attack on our systems, could result in a major data privacy or confidentiality breach causing damage to the customer experience and our reputational damage, a breach of regulations and financial loss."

Then, according to the SEC's Order, when the media learned of the breach and contacted the company, Pearson issued a misleading public statement downplaying the incident. Among other deficiencies, the SEC found that Pearson (1) inaccurately characterized the intrusion as "unauthorized access" when it was aware that the threat actor had actually removed data; (2) omitted to disclose that the removed data had included usernames and hashed passwords of employees; and (3) omitted to disclose that millions of rows of data were included in the breach. Notably, on the news, the company's stock price declined by only 3.3 percent.

Without admitting or denying the SEC's findings, Pearson agreed to settle the matter and pay a $1,000,000 penalty. In announcing the charges, Kristina Littman, Chief of the Enforcement Division's Cyber Unit, stated: "As public companies face the growing threat of cyber intrusions, they must provide accurate information to investors about material cyber incidents."

Lessons for public companies

The SEC's actions against First American and Pearson are notable for several reasons. First, neither case included any indication that the companies or their executives intended to deceive investors. It is also not clear that either cybersecurity incident was material to investors. Disclosure controls violations do not require a showing of materiality, and the SEC's Order in First American contained no reference to any impact on the company's stock price. In Pearson, although the company's stock price declined by only 3.3 percent, the SEC nevertheless found that the company made material misstatements and omissions. Given its questionable case on quantitative materiality, the SEC took pains in the Pearson Order to emphasize qualitative materiality factors, including that the company's reputation "depended in part on its ability 'to adequately protect personally identifiable information.'" The SEC's aggressive stance in these matters signals that there is a fine line between its view of conduct warranting enforcement action and its pledge not to "second-guess good faith exercises of judgment about cyber-incident disclosure."

Second, the Pearson case demonstrates that, when companies speak about cybersecurity incidents, they must carefully choose their words. The SEC found that Pearson made material omissions by failing to disclose all known features of the intrusion: while the company disclosed that email addresses and birth dates had been exposed, it failed to state that usernames and passwords of school personnel were affected. While these omitted features of the incident may not have been material in isolation, the SEC appears to be taking a broad view of materiality when companies fail to fully disclose all known facets of cybersecurity incidents.

Finally, Pearson underscores that public companies must exercise caution when crafting cybersecurity "risk factor" disclosures. The SEC found that Pearson misled investors by presenting the risk of a cybersecurity incident as hypothetical, when the company knew that the risk had already materialized. Yahoo, the SEC's first cybersecurity enforcement action, relied on the same theory. The SEC's scrutiny of cybersecurity disclosures underscores the need for public companies with awareness of past intrusions and vulnerabilities to carefully assess materiality and consider updates to their risk factors. These disclosures present significant real-world challenges given that just about every public company encounters cyber vulnerabilities and intrusions in some form or another.

Contributors

Luke Cadigan
Bio
