August 30, 2021

SEC Advances Broad Theory of Required Disclosures of Security Incidents

Attorneys
Fran Faircloth
Nameir Abbas

A recent SEC settlement has again demonstrated the Commission's continued attention to public companies' disclosures of cybersecurity incidents and its commitment to a broad notion of what constitutes such an incident. On August 16, the SEC entered a settlement agreement with Pearson plc, a UK-based educational publishing company that is publicly traded on both the London Stock Exchange and New York Stock Exchange via ADRs. While Pearson made no admissions in the agreement, it will pay a $1 million civil penalty to settle the SEC's allegations that Pearson misled investors in its disclosures related to a 2018 cybersecurity breach.

Five key aspects of this settlement merit attention from a cybersecurity perspective because they are arguably more aggressive than the practices that have developed under state data breach laws:

- The breach appears to have involved primarily usernames and hashed passwords, but the SEC did not appear to treat hashed passwords differently than un-hashed passwords.
- The SEC focused on the presence of birth dates and email addresses in a significant percentage of the records, even though many state laws do not consider loss of such information to constitute a reportable data breach.
- The SEC suggested that a typical affirmation of cybersecurity as a value was misleading: "Protecting our customers' information is of critical importance to us. We have strict data protections in place and have reviewed this incident, found and fixed the vulnerability."
- The SEC likewise suggested a statement that is typically made when there is no direct evidence of misuse to be misleading: "While we have no evidence that this information has been misused, we have notified the affected customers as a precaution."
- The SEC's Order also considered the "breach at issue [to be] material" because the business of the company involved collecting large amounts of private data about children – without any reference to the direct financial impact of the breach on Pearson.

This enforcement action follows a series of statements and enforcement actions from the Commission stressing the importance of cybersecurity disclosures. Many public companies began including cybersecurity as a risk factor in their public disclosures after the SEC Division of Corporation Finance issued guidance on such disclosures in October 2011. In February 2018 guidance, the Commission again addressed the disclosure of cybersecurity risks and events. In that statement, the SEC stressed the importance of "accurate and timely disclosures of material events." Only two months later, in April 2018, the SEC settled charges with Yahoo! for failing to disclose a 2014 data breach until 2016. Between 2018 and 2021, there were no further settlement agreements related to disclosure of cybersecurity events, but earlier this summer, the SEC showed renewed interest in the area, settling charges against First American Financial Corporation for alleged disclosure controls and procedures violations related to a cybersecurity vulnerability that potentially exposed customer information. The settlement with Pearson shows that such enforcement actions are likely to continue.

Incident Background and Impacted Data

On July 19, 2019, Pearson mailed a breach notification letter to customer accounts whose student and school personnel data had been impacted by a cybersecurity incident that began in November 2018. In that letter, Pearson said that affected data included student names, dates of birth, and email addresses, as well as administrator names, job titles, work

emails, and work addresses. On July 31, 2019, after being contacted by media, Pearson posted a public statement to its website, which said that "exposed data was isolated to first name, last name, and in some instances may include date of birth and/or email address." The day after Pearson's online statement about the incident, its NYSE stock price declined by 3.3% (although the broader markets were down roughly 1% that day as well).

According to the settlement, the cyber-intrusion that Pearson experienced in 2018 involved the theft of "several million" rows of student and school personnel data, across approximately 13,000 customer accounts in the United States. The intrusion exploited an unpatched vulnerability on a server relating to a Pearson product called AIMSweb 1.0, used to track and enter student academic performance details (a new version of the product called AIMSweb Plus was not affected). The settlement alleges that Pearson received notice of a patch for the vulnerability in question months prior to the intrusion but failed to implement the patch until afterward.

In addition, the settlement alleges that school personnel usernames and hashed passwords for the product were also affected by the incident, which was not disclosed in the notification letter or in the statement on Pearson's website.

Disclosures and Public Statements

On its Form 6-K published on July 26, 2019, which covered the first six months of 2019, Pearson did not mention the incident, instead issuing only the same general, *hypothetical* risk statement that it had issued on prior Forms 6-K: "[r]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" (emphasis added). Only five days later, on July 31, Pearson posted its online statement about the incident, prompting a drop in stock prices.

The SEC said that Pearson's general statement was insufficient to disclose that an actual breach had occurred. According to the settlement, Pearson failed to consider how that breach could have a material impact on its business that needed to be disclosed in its Form 6-K—especially given Pearson's recognition that it stored of "large volumes of personally identifiable information," including information about children. The settlement stated that a failure of Pearson's procedures led to the inadequate disclosures because the SEC considered the breach to be "material."

The SEC also took issue with alleged failures to

- Mention the loss of usernames and hashed passwords, in part because the hash at issue was an older and alleged unreliable hash algorithm. This is particularly noteworthy because many entities treat hashed data as equivalent to encrypted data (whose loss need not be disclosed), and the state laws with that exemption have generally not specified a particular strength for encryption or hashing methods.

- Mention that birth dates and email addresses were taken even though they were taken for certain records.

- Temper the general statement: "Protecting our customers' information is of critical importance to us. We have strict data protections in place and have reviewed this incident, found and fixed the vulnerability."

- To note circumstantial evidence of misuse based on the identity of the attacker, even though there was no direct evidence of misuse.

- Consider the breach to be "material" given that the company's business involved collecting large amounts of private data about children.

Takeaways

Pearson is the third such settlement related to this issue from the Commission. In each of these settlements, as in its 2018 guidance, the SEC has stressed the importance of adequate disclosure controls and procedures, which are necessary to enable public companies to make timely disclosure of cybersecurity incidents.

The SEC appears to be pursuing an approach to data breach disclosures that is significantly more aggressive than is required under state data breach laws. Given the SEC's focus, it will be important for public companies to be particularly robust in their disclosures of data breaches and to avoid typical reassuring statements in their data breach disclosures unless those are fully supported in the circumstances.

In the Pearson settlement, the SEC noted that "Pearson's processes and procedures around the drafting of its July 26, 2019 Form 6-K Risk Factor disclosures and its July 31, 2019 media statement failed to inform relevant personnel of certain information about the circumstances surrounding the breach." The Pearson settlement is a reminder that controls and procedures are necessary to ensure that the individuals who are in charge of issuing disclosures have the necessary information to meet their obligations. Public companies would be wise to assess how incidents are reported to key personnel involved in disclosure-related decisions and evaluate whether additional controls or procedures could help to provide appropriate and timely reporting.