GIBSON DUNN

# SEC Settlement Reflects Increasing SEC Focus on Cyber Disclosures

Client Alert | August 23, 2021

---

On August 16, 2021, the U.S. Securities and Exchange Commission announced a settled enforcement action against Pearson plc, a U.K. educational publisher, for inadequate disclosure of a cyber intrusion. According to the settlement, following a cyberattack, which the SEC deemed to be material, Pearson failed to revise its periodic cybersecurity risk disclosure to reflect that it had experienced a material data breach. In addition, in a subsequent media statement, Pearson misstated the significance of the breach by minimizing its scope and overstating the strength of the company's security measures. The settlement, in which Pearson agreed to pay a $1 million penalty, is the latest indication of the SEC's continuing focus on cyber disclosures as an enforcement priority and an important signal to public companies that, particularly in the face of an environment of increasing cyberattacks, accurate public disclosure about cyber events and data privacy is critical. The SEC action also underscores the importance, as part of an overall cyber-incident response, of carefully making materiality judgments.

According to the SEC Order,[1] Pearson learned in March 2019 that a sophisticated attacker took advantage of a vulnerability in software that Pearson provided to 13,000 school, district, and university accounts to access and download user names and passwords that were protected with an outdated algorithm as well as more than 11 million rows of student data that included names, dates of birth, and email addresses. The software manufacturer had publicized the existence of the vulnerability in September 2018 and made a patch available at that time; however, Pearson did not install the patch until after learning about the breach in March 2019. Also, at that time, Pearson conducted an internal investigation and began notifying impacted customers in July 2019.

According to the SEC Order, Pearson determined that it was not necessary to issue a public disclosure of the incident. The company's next report on Form 6-K contained the same data security risk disclosure that it had used in previous reports, stating that there was a "[r]isk" that "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). Consistent with its past position that companies should not discuss risks as hypothetical if they have already materialized or are materializing,[2] the SEC viewed this statement as implying that no "major data privacy or confidentiality breach" had occurred, and determined it was therefore misleading.

A few days after it filed this Form 6-K, a journalist asked Pearson about the data breach. In response, Pearson provided a statement, which it later posted on its website, that the SEC also described as misleading. According to the SEC Order, the statement had been prepared months earlier and failed to disclose that the attacker had extracted data, not just accessed it; understated what types of data were taken; suggested that it was uncertain whether data had been taken, whereas Pearson by that time allegedly knew exactly what data had been extracted; did not state how many rows of data were involved; and stated that Pearson had "strict data protections" and had patched the vulnerability, even though Pearson had waited months to install the patch and had relied upon outdated software to

### Related People

Mark K. Schonfeld

Lori Zyskowski

Thomas J. Kim

Ronald O. Mueller

Terry Wong

encrypt passwords.

As a result of the foregoing statements, the SEC Order states that Pearson violated Sections 17(a)(2) and (a)(3) of the Securities Act, provisions which prohibit misleading statements or omissions in the context of a securities offering,[3] as well Section 13(a) of the Exchange Act. The SEC Order also finds that the conduct demonstrated that Pearson failed to maintain adequate disclosure controls and procedures in violation of Exchange Act Rule 13a-15(a).

The *Pearson* settlement reflects a number of instructive points. First, this settlement demonstrates the importance of carefully assessing the materiality of a cyberattack. Here, the SEC determined that the data breach was material based on, among other things, the company's business and its user base, the nature and volume of the data exfiltrated, and the importance of data security to the company's reputation, as reflected in the company's existing risk disclosures. However, the order does not assert that there was any adverse impact on Pearson's business as a result of the incident. In fact, Pearson's subsequent filings on Form 20-F expressly stated that prior attacks "have not resulted in any material damage" to the business. Consulting with counsel in making materiality assessments can help mitigate the risk of the government second-guessing materiality judgments in hindsight. Second, this is the third recent enforcement case that the SEC has brought based on disclosures contained in reports that are "furnished," not "filed" with the SEC and in media statements.[4] Third, this is the second enforcement case in which the SEC has found that a company's disclosures regarding a cybersecurity incident reflected inadequate disclosure controls and procedures.[5] Collectively, these cases reiterate that the SEC is intensely focused on cybersecurity disclosure issues, that public companies should be mindful of SEC disclosure considerations when responding to or publicly commenting on a cybersecurity issue, and that companies should ensure that their disclosure controls and procedures appropriately support their cybersecurity response plans.

The *Pearson* settlement is the latest — and likely not the last — SEC cyber disclosure enforcement action. The SEC Enforcement Division has also taken an expansive look into cyber disclosures with a sweep related to how companies responded to the widely reported SolarWinds breach, where foreign hackers believed to be tied to Russia used SolarWinds' software to breach numerous companies and government agencies.[6] The agency asked companies it believed were impacted to voluntarily furnish information about the attack, and offered immunity, under certain conditions, for potential disclosure failings.[7]

In addition, although SEC interpretive guidance on cybersecurity disclosures was issued in 2018,[8] additional disclosure rulemaking appears likely. According to the Unified Agenda of Regulatory and Deregulatory Actions ("Reg Flex Agenda") made available in June 2021, the first reflecting Chair Gary Gensler's agenda,[9] the SEC is considering whether to propose new rules to enhance issuer disclosure on "cybersecurity risk governance."[10]

The possible new proposed rulemaking project and the increasing enforcement efforts are a clear signal of the SEC's continuing focus on accurate cybersecurity disclosures and robust disclosure controls and procedures around cybersecurity. The recent increase in cyberattacks contributes to the focus, as does the apparent perception of a risk that companies may under-report data security incidents. The *Pearson* enforcement action makes plain that a company's disclosure about the *possible* risk of a data breach will likely be insufficient — and even be viewed as misleading — if the company has in fact suffered a cyber breach that the SEC deems to be material. Moreover, the SEC's actions reinforce the importance of having strong disclosure controls and procedures so that full information about data breaches and vulnerabilities are communicated to those making decisions about disclosures.

---

[1] *In re Pearson plc*, Release No. 33-10963 (Aug. 16, 2021), https://www.sec.gov/litigation/admin/2021/33-10963.pdf.

[2] *See* Gibson, Dunn & Crutcher, "Considerations For Preparing Your 2019 Form 10-K" (Jan. 13, 2020), https://www.gibsondunn.com/considerations-for-preparing-your-2019-form-10-k; Gibson, Dunn & Crutcher, "Considerations For Preparing Your 2020 Form 10-K" (Feb. 3, 2021), https://www.gibsondunn.com/considerations-for-preparing-your-2020-form-10-k.

[3] These violations, which the SEC Order notes do not require a showing of intent, appear to be premised on the fact that Pearson had employee benefit plan equity offerings on-going that were registered on a Form S-8.

[4] *See also In re First American Financial Corp.*, Release No. 34-92176 (June 14, 2021), https://www.sec.gov/litigation/admin/2021/34-92176.pdf; *The Cheesecake Factory Incorporated*, Release No. 34-90565 (Dec. 4, 2020), https://www.sec.gov/litigation/admin/2020/34-90565.pdf (disclosure involved two "furnished" Form 8-Ks).

[5] *In re First American Financial Corp.*, Release No. 34-92176 (June 14, 2021), https://www.sec.gov/litigation/admin/2021/34-92176.pdf. In the First American Financial Corp. case, the SEC Order alleged that company executives did not have full information about a cybersecurity vulnerability when the company issued a statement to a reporter and furnished a voluntary Form 8-K addressing the situation. *Id.*

[6] Katanga Johnson, "U.S. SEC probing SolarWinds clients over cyber breach disclosures -sources," Reuters (June 22, 2021), https://www.reuters.com/technology/us-sec-official-says-agency-has-begun-probe-cyber-breach-by-solarwinds-2021-06-21.

[7] In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs, U.S. Sec. & Exch. Comm'n, https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs (last modified June 25, 2021).

[8] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166 (Feb. 26, 2018), https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf.

[9] Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Annual Regulatory Agenda (June 11, 2021), https://www.sec.gov/news/press-release/2021-99.

[10] *See* Gibson, Dunn & Crutcher, "Back to the Future: SEC Chair Announces Spring 2021 Reg Flex Agenda" (June 21, 2021), https://www.gibsondunn.com/back-to-the-future-sec-chair-announces-spring-2021-reg-flex-agenda.

---

This alert was prepared by Alexander H. Southwell, Mark K. Schonfeld, Lori Zyskowski, Thomas J. Kim, Ron Mueller, Eric M. Hornbeck, and Terry Wong.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work in the firm's Privacy, Cybersecurity and Data Innovation, Securities Regulation and Corporate Governance, and Securities Enforcement practice groups, or the following authors:

Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Mark K. Schonfeld – New York (+1 212-351-2433, mschonfeld@gibsondunn.com)
Lori Zyskowski – New York (+1 212-351-2309, lzyskowski@gibsondunn.com)
Thomas J. Kim – Washington, D.C. (+1 202-887-3550, tkim@gibsondunn.com)
Ronald O. Mueller – Washington, D.C. (+1 202-955-8671, rmueller@gibsondunn.com)
Eric M. Hornbeck – New York (+1 212-351-5279, ehornbeck@gibsondunn.com)

GIBSON DUNN



## Related Capabilities

Privacy, Cybersecurity, and Data Innovation

Securities Regulation and Corporate Governance

Securities Enforcement