**Dan Goelzer**

# AUDIT COMMITTEE AND AUDITOR OVERSIGHT UPDATE

Update No. 69
August 2021

This Update summarizes recent developments relating to public company audit committees and their oversight of financial reporting and of the company's relationship with its auditor.

### In This Update:



## Abuse of Audit Committee Auditor Selection Process Triggers an Independence Violation

The Securities and Exchange Commission has charged Ernst & Young (EY) and three of its former partners with violations of the auditor independence rules as a result of conduct that interfered with an audit committee's competitive bidding process for the company's audit engagement. The SEC also charged the company's former Chief Accounting Officer (CAO) with causing reporting violations based on his efforts to aid EY in obtaining the engagement. (While the SEC's orders do not name the company, prior SEC filings and press reports disclosed that it is Sealed Air, a North Carolina-based manufacturer of packaging material. The company was not charged.)

SEC Findings

According to the SEC's order, the CAO, while employed at another company, worked with one of the EY partners and viewed him as a "trusted adviser." In 2013, the CAO was hired by Sealed Air and became

---

Dan Goelzer is a retired partner of a major global law firm. He is a member of the Sustainability Accounting Standards Board and advises a Big Four accounting firm on audit quality issues. From 2002 to 2012, he was a member of the Public Company Accounting Oversight Board and served as Acting PCAOB Chair from August 2009 through January 2011. From 1983 to 1990, he was General Counsel of the Securities and Exchange Commission.

involved in discussions about initiating a solicitation for bids to perform its audit. The audit committee authorized an RFP and invited EY and three other firms, including the incumbent auditor, to submit bids.

The SEC finds that the audit committee intended to conduct a competitive and fair RFP process. The RFP stated that firms would have an "equal opportunity to provide their best proposals" to the committee, that information submitted by firms would be treated as confidential, and that "all competitors that submitted proposals represented that: (i) Issuer personnel have not participated in the preparation of the firm's proposal; and (ii) Issuer personnel have not conveyed to the competitors any information pertaining to this RFP."

Despite the audit committee's intentions, and unknown to the committee, the CAO provided EY with confidential information and other assistance. In particular, the CAO furnished EY, through the partner with whom he had previously worked, with the other firms' proposals and submissions and with the internal documents prepared for the audit committee. For example:

- The CAO sent EY a slide deck that he planned to present to the audit committee on the pros and cons of each bid and asked for "additional talking points that you think might be beneficial." After consultation with other EY partners, the partner with whom the CAO had previously worked provided CAO with a detailed list of additional "cons" against the incumbent audit firm.

- The audit committee selected EY and the incumbent firm as finalists and gave each a deadline to submit final bids. The CAO forwarded the incumbent firm's final bid to two EY partners. Five days later – and after the audit committee's deadline -- EY submitted its final bid, which was almost identical to the incumbent's, but slightly higher when expenses were taken into consideration. The CAO deleted the expenses from the final bid summary provided to the audit committee, creating the appearance that EY's bid was lower.

Unaware of these matters, the audit committee selected EY as its new auditor. Sealed Air thereby became EY Charlotte's largest audit client. On the evening the selection was announced, the CAO sent an EY partner (his former college roommate), a congratulatory email with the message: "Back in the family!!!"

In connection with the 2015 and 2016 annual audits, the EY engagement partner signed letters to the audit committee purporting to disclose, as required by PCAOB rules, all matters that could reasonably bear on EY's independence. These letters did not disclose EY's or the CAO's conduct related to the RFP.

Analysis

Under its auditor independence rule, the SEC will not recognize an accountant as independent "if the accountant is not, or a reasonable investor with knowledge of all relevant facts and circumstances would conclude that the accountant is not, capable of exercising objective and impartial judgment on all issues encompassed within the accountant's engagement." In its order, the SEC finds that a reasonable investor with knowledge of all the facts and circumstances concerning the RFP process would conclude that the three EY partners involved were not capable of exercising objective and impartial judgment regarding Sealed Air's 2015 audit. An individual accountant's lack of independence may be attributed to the firm in which the auditor practices. Therefore, the SEC also finds that a reasonable investor with knowledge of all relevant facts and circumstances would conclude that EY was not capable of exercising objective and impartial judgment.

On this basis, the SEC finds that EY violated the auditor independence rules, that the three former partners caused that violation, and that the firm and its partners caused Sealed Air to violate certain SEC reporting requirements. The CAO aided and abetted the reporting violations.

Settlement and Sanctions

EY and the individuals all agreed to settle without admitting or denying the Commission's findings. EY was censured, agreed to pay a fine of $10 million, and undertook to comply with various procedures to prevent

future violations. The three former EY partners, and the former CAO, were barred from practicing before the Commission and agreed to fines ranging from $15,000 to $51,000.

Comment: This case involved a deliberate effort by the CAO, with the knowledge of his preferred accounting firm, to mislead the audit committee and to undermine its competitive selection process. It is difficult for audit committees to anticipate and defend against this kind of abuse of trust. While this type of situation is – hopefully – rare, the case is a reminder that management may have an undisclosed bias in favor of a particular firm and that the audit committee should be vigilant to protect its decision-making against the effects of such bias.

Another point illustrated by this case is that the audit committee is dependent on the information it receives about issues that may impact independence. While the auditor is normally the primary source of such information, management needs to be involved as well. The audit committee should set an expectation with management that it will inform the audit committee of any prior, unusual, or new relationships between the auditor and senior members of management, especially those involved in financial reporting. In this connection, company staff that interact with the auditor should have some basic understanding of the principles of auditor independence so that they will be sensitive to issues that could impact the reasonable investor's view of auditor objectivity and impartiality.

## SEC Takes a Dim View of Sugar-Coating Cybersecurity Breaches

On August 16, the Securities and Exchange Commission announced an enforcement action against Pearson plc, a company that provides educational publishing and other services to schools and universities. The SEC's order finds that Pearson misled investors about a 2018 cyber intrusion. The case is a reminder of the disclosure implications of cybersecurity breaches and of the risks of failing to promptly inform investors of such incidents or downplaying their severity. It also highlights the importance of regularly reviewing risk factor disclosure and of not repeating the same risk disclosure as in prior filings when the underlying facts have changed.

Facts

Pearson is a U.K. company with shares traded on the London Stock Exchange and American Depository Receipts listed on the New York Stock Exchange. Among the services it offers to educational institutions is web-based software for entering and tracking students' academic performance.

According to the SEC's order, on March 21, 2019, Pearson learned that data stored on one of its servers had been accessed and downloaded by a hacker who exploited an unpatched server vulnerability. Although the server software manufacturer had publicized the vulnerability six months earlier and issued a patch, Pearson did not implement the patch until after it learned of the attack. As a result of the breach, the intruder obtained millions of student records, including birthdates and email addresses, along with school district personnel usernames and weakly encrypted passwords. Pearson mailed a breach notice to the affected customers but concluded that no public disclosure was necessary.

On July 25, 2019, Pearson furnished to the SEC a report on Form 6-K of its results for the first six months of 2019. In the "Principal risks and uncertainties" section of that report, Pearson stated that a "[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) The same statement had appeared in its prior Forms 6-K.

On July 31, a reporter informed Pearson that an article would soon be published revealing the data breach. That evening, Pearson posted a statement on its website regarding the breach. The SEC finds that this statement was misleading in several respects, including –

- The statement described the incident as involving "unauthorized access" to data, when in fact Pearson was aware that the hacker had removed -- not merely accessed -- data from the compromised server.

- The statement said that the data in question "may include date of birth and/or email address" when in fact Pearson was aware that approximately half of the exfiltrated data contained birthdates and that approximately 290,000 contained email addresses.

- The statement asserted that "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." Pearson did not however reveal that the hacker obtained access to its server through a vulnerability of which Pearson had been notified and failed to patch for six months after notification.

Analysis

In the SEC's view, the Pearson cybersecurity breach was material for securities law disclosure purposes. The order explains:

> "The breach at issue was material because Pearson's business * * * involved collection and storage of large quantities of private data on school-age children around the world. As Pearson acknowledged in its risk disclosures, Pearson 'holds large volumes of personally identifiable information,' and its reputation and ability to attract and retain revenue depended in part on its ability 'to adequately protect personally identifiable information.' This breach involved a compromise of a server holding a large quantity of data Pearson was responsible for protecting * * *. It also involved lapses in Pearson's protection of that data."

The SEC also finds that Pearson's processes and procedures around the drafting of its July 26, 2019 Form 6-K disclosures and its July 31, 2019 public statement failed to inform company personnel responsible for disclosure of certain information about the circumstances surrounding the breach. "Although protecting student and user data is critical to Pearson's business, and Pearson had identified the potential for improper access to such data as a significant risk, it failed in this way to maintain disclosure controls and procedures designed to analyze or assess such incidents for potential disclosure in the company's filings."

On the basis of these findings, the SEC concludes that Pearson violated various provisions of the federal securities laws that prohibit untrue or materially misleading public statements or the furnishing of inaccurate or misleading information to the Commission. The company also violated SEC rules requiring the maintenance of disclosure controls and procedures designed to ensure the recoding of information required to be disclosed in reports filed with or furnished to the SEC.

Settlement and Sanctions

Without admitting or denying the SEC's findings, Pearson agreed to a cease-and-desist order prohibiting future violations and to payment of a civil money penalty of $1 million to settle the proceeding. The order notes that, in accepting the settlement, the SEC considered Pearson's cooperation with the SEC staff.

Comment: Pearson illustrates several points that audit committees should keep in mind if the company finds itself in the position of dealing with a cybersecurity breach or vulnerability.

- Cybersecurity disclosure is a top SEC priority. The Commission's staff is likely to scrutinize closely any public statement or filing concerning a cyber breach. In June, the SEC brought a case similar to Pearson in which it alleged that a financial institution's inadequate disclosure controls resulted in incomplete public statements and filings regarding a cybersecurity vulnerability. Additional cases of this nature are likely. Further, the Commission announced in June that the Division of Corporation Finance is considering rules to enhance issuer disclosures regarding cybersecurity risk governance. See The SEC's Agenda – ESG Tops the List, July

2021 Update. In light of this emphasis, disclosures related to cybersecurity matters need to be carefully drafted, preferably with input from experienced SEC counsel.

- In considering whether a breach is material for purposes of securities law disclosure, factors beyond the direct cost of the breach need to be weighed. As the Pearson order makes clear, in assessing materiality, the SEC will look to the potential impact on the company's reputation and future ability to attract revenue and to the company's responsibility to protect the privacy of third parties. Also, risk factor discussion of the importance of cybersecurity may be evidence of the materiality of a breach. The best approach may be to start with a presumption that any cybersecurity breach is material, unless the consequences are clearly trivial.

- If the company becomes aware of a breach, existing disclosures regarding cybersecurity risks should be reviewed and modified as necessary. Risk factor or other disclosures regarding the possibility that a cyber breach could occur are likely to be misleading after a breach does occur.

A key lesson of Pearson is the importance of well-thought-out disclosure controls and procedures. In both Pearson and the prior case mentioned above, a fundamental problem seems to have been that important information regarding a cyber vulnerability or breach was not fully communicated to those responsible for disclosure. In overseeing the effectiveness of the company's disclosure controls, the audit committee may want to consider whether the company's procedures recognize the importance of this line of communication.

## The S&P 500 Are (Almost) All in on ESG Disclosure

The Center for Audit Quality (CAQ) has published S&P 500 and ESG Reporting, a study of S&P 500 company environmental, social, and governance (ESG) disclosures. The CAQ found that 95 percent of S&P 500 companies publicly disclose detailed ESG information -- primarily in a standalone ESG, sustainability, corporate responsibility, or similar report, not in an SEC filing. Most of the remaining five percent publish "high-level policy information" on their website. About six percent of the S&P 500 received assurance from a public company auditing firm with respect to some part of their ESG disclosures, while about 47 percent obtained assurance from some other type of service provider.

During the past year, the CAQ has published several papers on the auditor's role in ESG reporting. See Want to Improve the Reliability of Your ESG Reporting? The CAQ Suggests Asking Your Auditor for Help, July-August 2020 Update and CAQ Provides Guidance on Auditor ESG Assurance, March-April 2021 Update. The new CAQ report looks broadly at the extent to which large companies are making ESG disclosures and the extent to which they are asking their auditors, or other service providers, for assurance on their ESG reporting.

Some highlights of the CAQ study include:

- ESG Reporting Period. Most of the S&P 500 report ESG information annually (or disclose their intension to report annually). As of June 18, 2021, 54 percent of S&P 500 companies had published ESG data for periods ending in 2020, while 37 percent had published data for periods ending in 2019.

- ESG Reporting Frameworks and Standards. The CAQ tracked references to five ESG disclosure frameworks or standards: CDP (formerly known as the Carbon Disclosure Project), the Global Reporting Initiative (GRI), the Sustainability Accounting Standards Board (SASB), the Task Force on Climate Change (TCFD) and Integrated Reporting (IR). The CAQ found that 459 of the 500 companies referenced at least one of these five reporting frameworks or standards in their disclosure, and almost 80 percent (390 companies) referenced more than one framework or standard. Ten companies referred to all five. The most frequently referenced ESG disclosure framework or standard was CDP (371 companies), followed closely by SASB (362 companies) and GRI (328 companies).

- Assurance or Verification. About 52 percent of the S&P 500 (264 companies) disclosed some form of third-party assurance or verification over all or part of their ESG metrics. Thirty-one of these companies retained an audit firm to provide assurance, while 235 utilized an engineering or consulting firm. (Two companies obtained assurance from both an accounting firm and some other type of service provider.)

- Scope of Assurance. The majority (123 of 229) of the ESG assurance reports issued by non-auditor service providers covered only greenhouse gas (GHG) emissions. In contrast, the majority (22 of 31) of the reports issued by public company auditors covered metrics other than, or in addition to, GHG. Only 10 percent of assurance or verification reports from non-auditors covered multiple areas.

- Assurance Standards. Of the 31 assurance reports issued on ESG disclosures by audit firms, 27 of the engagements were performed based on the attestation standards of the American Institute of Certified Public Accountants, and four were performed under the International Standard on Assurance Engagements. One engagement referenced both sets of standards, and the standards under which one engagement was performed were not publicly disclosed. The most common assurance standard that non-auditor service providers referenced was Organization for Standardization 14064-3 Green-house gases -- Part 3: Specification with guidance for the verification and validation of greenhouse gas statements (ISO 14064-3).

- Level of Assurance. Of the 31 companies that obtained ESG assurance from public company auditors, 25 obtained limited levels of assurance over select information. Three companies obtained limited assurance over some metrics and reasonable assurance over other metrics. Two companies obtained reasonable assurance as to all metrics that were reviewed. In one case, the level of assurance could not be determined from the company's disclosure. The great majority of reports issued by non-auditors provided limited assurance, although some used the terms "reasonable" or "moderate" or a mix of assurance levels.

The CAQ separately analyzed S&P 100 ESG disclosures. Among other things, the CAQ found that 82 percent of S&P 100 companies received some third-party assurance or verification over their ESG disclosures, compared to only 46 percent of the remaining S&P 500 companies. Further, 13 percent of the S&P 100 obtained such assurance from a public company auditor, as compared to less than five percent of the other 400 companies. The CAQ study shows that the SASB standards are rapidly gaining in popularity among the largest companies. Between March 12 and June 18, 2021, SASB overtook GRI as the second most referenced disclosure framework (apparently, after CDP) among the S&P 100.

Comment: The CAQ's findings are broadly consistent with those of the Governance & Accountability Institute regarding the rapid growth of large and mid-sized U.S. public company ESG disclosure. See G&A Finds That Ninety Percent of the S&P 500 Publish a Sustainability Report, July-August 2020 Update and With Sustainability Reporting on the March, Protiviti Has Ten Questions Directors Should Ask, October-November 2020 Update. One of the themes of the Update has been that audit committees need to be aware of this ESG disclosure revolution. Sustainability disclosures are increasingly relied upon in investor decision-making and recognized as material for purposes of the federal securities laws. However, ESG disclosures are often not subject to the same controls and procedures as apply to traditional financial disclosures. This creates risks that the sustainability report may be inconsistent with other company disclosures or that the accuracy of the information presented may not be verifiable. These risks should be of concern to audit committees because of their responsibility for disclosure oversight and for related controls and procedures.

Auditor (or other third-party) assurance with respect to ESG disclosure can be an important tool in promoting confidence in ESG reporting. The CAQ report make clear that assurance is becoming more common and -- indeed might be viewed as the norm among the largest companies. Managements and audit committees that are not already doing so should give serious consideration to obtaining assurance over disclosures that include ESG metrics. In its publications, the CAQ makes a strong case for retaining the financial statement auditor to provide this assurance. Audit committees considering whether to retain their auditor or another type of professional to provide ESG assurance need to weigh a variety of factors, including each candidate's

reputation, independence, relevant expertise, and familiarity with the company and its systems. The professional standards an assurance provider applies are also a key factor.

## On the Update Radar: Things in Brief

**The Auditor's Responsibilities for Detecting Illegal Client Acts.** The Center for Audit Quality has released, Illegal Acts: The External Auditor's Responsibilities. This publication provides an overview of the auditor's responsibilities under the PCAOB's auditing standards with respect to illegal acts and how those responsibilities differ from the auditor's responsibility to detect fraud. The auditor's responsibility for illegal acts is often misunderstood, and the CAQ's publication provides a useful introduction to the topic for audit committee members and others.

The PCAOB's auditing standards require the auditor to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. In contrast, the PCAOB's standards normally do not require auditors to perform procedures designed to detect illegal acts. However, the performance of audit procedures may bring possible illegal acts to the auditor's attention. When that happens, the auditor is required to obtain an understanding of the nature of the illegal act, the circumstances in which it occurred, and other information to evaluate any effect on the financial statements. The CAQ states that, in general, the potential impact of an illegal act on the financial statements falls into one of three categories:

- The possible illegal act is not directly material to the financial statements and is not likely to have an indirect material financial statement impact (e.g., a company employee accepted a bribe from a supplier). Illegal acts that are immaterial to the financial statements may nonetheless raise audit-related issues concerning such matters as the company's internal controls and ethical culture.

- The possible illegal act is not directly material to the financial statements, but could have a material indirect impact (e.g., the illegal act requires consideration of the need for a loss contingency).

- The possible illegal act has a direct material impact on the financial statements, requiring the auditor to respond as in the case of any material misstatement.

While outside the scope of the CAQ publication, audit committees should also be aware that Section 10A of the Securities Exchange Act imposes certain requirements on public company auditors with respect to illegal acts. Section 10A provides that financial statement audits "shall include * * * [p]rocedures designed to provide reasonable assurance of detecting illegal acts that would have a direct and material effect on the determination of financial statements amounts." In addition, the Act requires that, whenever an auditor becomes aware that an illegal act may have occurred, regardless of impact on the financial statements, the auditor must inform the appropriate level of the management and assure that the audit committee (or the board of directors in the absence of an audit committee) is notified. In the case of an illegal act that has a material financial statement impact, if management and the board fail to take "timely and appropriate remedial action", the auditor must report to the SEC.

**Accounting Quality Alarm Bell: Changes in Accounting Estimates**. In a recent blog post, research and data provider Audit Analytics notes that changes in accounting estimates (CAEs) "can be a significant accounting quality red flag." Changes in estimates are inherently judgmental, and management has considerable latitude in deciding the timing and amount of such adjustments. As AA observes, "Management is able to use its own discretion in determining appropriate estimates for calculating the value of many accounts, like property, plant, and equipment."

AA cites studies that show that changes in accounting estimates frequently indicate poor quality accounting. For example, in Mandatory Disclosure and Management Discretion: On the Case of

Changes, Anne Albrecht (Neeley School of Business, Texas Christian University), Kyonghee Kim (Eli Broad College of Business, Michigan State University) and Kwang J. Lee (KAIST College of Business, Korea Advanced Institute of Science and Technology) characterize changes in accounting estimates as "an additional measure of earnings management." These authors state that "managers tend to implement a positive CAE when it helps meet or beat earnings benchmark and a negative CAE when it is unlikely to cause a negative earnings surprise." Moreover, they find that "financial reports containing CAEs are more likely misstated and subject to the SEC inquiries."

AA concludes its analysis with this observation: "Changes in accounting estimates can carry significant risks. CAEs can lower financial reporting quality, as well as affect projections of future earnings. When CAEs are disclosed, they should be noted and carefully analyzed by investors." Audit committees may want to consider taking the same approach and making sure that they understand the basis and motivation for any changes in estimates.

## The Audit Blog

I am a co-founder of The Audit Blog and blog on developments in auditing and financial reporting, on auditor oversight and regulation, and on sustainability disclosure. Occasionally, items that appear in the Audit Committee and Auditor Oversight Update also appear on the blog. Recent posts include --

- The Housecleaning at the PCAOB: Why it Matters (Dan Goelzer, July 6, 2021)

The blog is available here. You can follow it @BlogAuditor on twitter or @the-audit-blog on medium.com.

**For further information, please contact**:

Daniel L. Goelzer
301.288.3788
dangoelzer@gmail.com

Email distribution of the Update is provided free of charge. If you would like to be added to the distribution, please email me at the address above. Readers are also free to recirculate the Update.

The Update seeks to provide general information of interest to audit committees, auditors, and their professional advisors, but it is not a comprehensive analysis of the matters discussed. The Update is not intended as, and should not be relied on as, legal or accounting advice.

Prior Updates issued between January 1, 2019, and May 31, 2020, are available here. Updates issued after June 1, 2020, are available here.