Update

No. 27
February-March 2016

AUDIT COMMITTEE AND AUDITOR OVERSIGHT UPDATE

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:

SEC Enforcement Remains Focused on Financial Reporting and its Gatekeepers

FASB Adopts New Lease Accounting Standard

SEC Shareholder Proposal Rule Can't Be Used to Force Audit Committees to Put the Audit Out for Bids

Auditors that Prepare the Corporate Tax Return Tend to Do So Cautiously

Cybersecurity Risk Now Tops Public Company Directors' Worries, With Reputational Risk Close Behind

Investors Don't Reward Candor About Cyber Risk – But the SEC Might

Prepared by:

Daniel L. Goelzer

+1 202 835 6191
Daniel.Goelzer@bakermckenzie.com

SEC Enforcement Remains Focused on Financial Reporting and its Gatekeepers

In his January 25 keynote address, SEC Enforcement Director Andrew Ceresney told attendees at the 2016 Directors Forum in San Diego that, since 2013, the agency has significantly increased the quality and number of its financial reporting cases. Moreover, the emphasis on financial reporting will continue because "significant violations still occur, accounting frauds are still perpetrated, and gatekeepers still fail to comply with their legal and professional obligations." Therefore, he warned, "audit committee members who fail to reasonably carry out their responsibilities, and auditors who unreasonably fail to comply with relevant auditing standards in their audit work, can expect to be in our focus."

Mr. Ceresney stated that, with respect to financial reporting enforcement generally, "the Commission has more than doubled its actions in the issuer reporting and disclosure area – from 53 in fiscal year 2013 to 114 in fiscal year 2015." In most of these actions, individuals, often senior executives have been charged, along with the reporting company. "During the past two fiscal years, excluding follow-ons, the Commission has charged over 175 individuals in issuer reporting and disclosure matters."

Mr. Ceresney listed five specific aspects of financial reporting that have triggered SEC enforcement:

- Revenue Recognition. "Improper revenue recognition continues to be an area in which [we] see manipulation and wrongdoing, largely because revenues are such a critical measure of performance."

- Valuation and Impairment Issues. "In the last several years, valuation and impairment issues also have been a prominent theme in many of the Commission's financial reporting enforcement actions, in some cases relating to actions arising during the financial crisis which produced unusual impacts on assets. * * * Particularly in times of economic turmoil, when valuation adjustments and management discretion may be the last avenues for improperly enhancing performance, we look closely at these issues."

- Earnings Management. "Managing earnings and other financial targets was obviously a hallmark of some of the major accounting cases in the early 2000s. And this is an area where the Commission has continued to see issues."

- Missing or Insufficient Disclosures. "[M]issing or insufficient material disclosures hinder investors' ability to make informed investment decisions. These deficient disclosures have ranged from executive perks to related party disclosures."

- Internal Accounting Controls. "In addition to financial statement and disclosure issues, we have also been focused on deficient internal accounting controls, which are foundational to reliable financial reporting. On a number of occasions, we have brought charges for violations of the internal accounting controls provisions of the federal securities laws, even in the absence of fraud charges. Deficient internal accounting controls can lay the groundwork or create opportunity for future misstatement or misconduct that goes undetected."

He also noted that the Commission has "aggressively" used its authority under the Sarbanes-Oxley Act to "claw back" compensation from executives of companies that have engaged in financial reporting violations that resulted in restatements.

Mr. Ceresney emphasized, as has SEC Chair Mary Jo White (see July 2014 Update), that audit committee members, along with external auditors, are gatekeepers whose role is "critical to helping ensure that issuers make timely, comprehensive, and accurate disclosure" and who have "a responsibility to foster high-quality, reliable financial reporting." However, as to audit committee members in particular, Mr. Ceresney suggested that their inclusion in financial reporting enforcement actions was the exception, not the rule:

> "We have not frequently brought cases against audit committee members. That is because in my experience, audit committee members in most cases carry out their duties with appropriate rigor. But in the last couple of years, we have brought three cases against audit committee chairs that provide helpful guidance on the type of failures that will attract our attention. In each case, the audit committee member approved public filings that they knew, were reckless in not knowing, or should have known were false because of other information available to them."
>
> * * *
>
> "The takeaway from these cases is straightforward: when an audit committee member learns of information suggesting that company filings are materially inaccurate, it is critical that he or she take concrete steps to learn all relevant facts and cease annual and quarterly filings until he or she is satisfied with the accuracy of future filings."

The three audit committee member cases to which Mr. Ceresney referred are –

- AgFeed Industries (see April 2014 Update) (audit committee chair allegedly learned facts suggesting that sales were inflated and was advised by a former director that there was "not just smoke but fire" and that an internal investigation was warranted; the audit committee chair allegedly ignored these warnings and signed off on the filing of the financial statements).

- L&L Energy (see April 2014 Update) (in a settled case, former audit committee chair was found to have signed an annual report that she knew or should have known contained a certification purportedly signed by the company's acting CFO when, in fact, the person identified as acting CFO had declined to serve in that position).

- MusclePharm (see September 2015 SEC order) (in a settled case, former audit committee chair was found to have signed several SEC filings that did not disclose the full extent of executive perquisite compensation; although audit committee chair learned of the nondisclosure of the perks, according to the order, he substituted his interpretation of the disclosure requirements for the views of the company's compensation consultant, resulting in additional filings with incomplete perks disclosure).

Comment: Director Ceresney's comments make clear that the SEC's focus on financial reporting and its "Operation Broken Gate" (see October 2013 Update), under which auditors and directors may be held responsible for financial reporting failures, will continue in full swing, at least through the end of SEC Chair White's term. Audit committee members can take some comfort from his assertions that enforcement cases alleging that directors bear responsibility for these violations are rare and will only be initiated when the director knew or should have known that the company was filing inaccurate information with the SEC. However, while the cases that have been brought during the last several years seem fairly clear-cut, it is easy to imagine situations in which it may be more debatable whether audit committee members "should have known" of the company's reporting violation.

FASB Adopts New Lease Accounting Standard

On February 25, the Financial Accounting Standards Board adopted ASU No. 2016-02, Leases (Topic 842), which establishes new principles governing financial reporting about the assets and liabilities that arise from leases. The standard, which has been under consideration since 2006, is summarized in the December 2015 Update. It will require lessees to recognize assets and liabilities for leases with terms of more than 12 months and will affect the financial statements of virtually all companies that lease assets. For public companies, the ASU will take effect for fiscal years, and interim periods within those fiscal years, beginning after December 15, 2018. For all other organizations, it is effective for fiscal years beginning after December 15, 2019, and for interim periods within fiscal years beginning after December 15, 2020.

In the press release announcing adoption of the new guidance, FASB Chair Russell G. Golden stated that the leasing ASU "responds to requests from investors and other financial statement users for a more faithful representation of an organization's leasing activities." Further, it

"ends what the U.S. Securities and Exchange Commission and other stakeholders have identified as one of the largest forms of off-balance sheet accounting, while requiring more disclosures related to leasing transactions." In a paper entitled Understanding Costs and Benefits, the Board states that the new guidance will result in "fewer opportunities for organizations to structure leasing transactions to achieve a particular accounting outcome on the statement of financial position" and will improve "understanding and comparability of lessees' financial commitments regardless of how the lessee finances the assets used in its businesses."

However, as the Costs and Benefits paper acknowledges, some companies may face significant implementation costs and challenges. "For example, organizations will, in general, incur initial costs to educate employees about how to apply the new requirements, and to explain to users the effects of the changes in accounting for leases on the organization's financial statements. In addition, many organizations may need to consider supplemental processes and controls to ensure that they capture leasing activity on the balance sheet."

Comment: Companies that engage in any significant amount of leasing should analyze the challenges that the new standard will pose and formulate an implementation plan as soon as possible. Some of the issues that the audit committee may want to raise with management include –

- The need for new data collection, storage, and maintenance processes. Companies will need to create a data base of their existing leases – something that they may not have found necessary under the current accounting regime – and determine the assets and liabilities arising from those leases after the ASU becomes effective. Procedures will also have to be put in place to capture this information for future leases.

- The need for IT upgrades. The new data collection, retention, and processing needs may require changes in the information technology that supports leasing activity.

- Changes in internal controls. In light of the Securities Exchange Act internal control requirement and Sarbanes-Oxley Act assessment and auditing requirements for internal control over financial reporting, as new processes are created to comply with the leasing standard, it will be necessary to make sure that those processes are consistent with the company's control framework and are operating effectively.

- The impact on debt covenants and financial ratios. The inclusion of lease assets and liabilities on the financial statements will affect traditional financial measures, such as the debt-to-equity ratio and return on total assets. It may be necessary to renegotiate loan covenants with existing lenders to avoid breaches resulting from these changes. The impact of the new standard will also need to be taken into account in future loan negotiations.

SEC Shareholder Proposal Rule Can't Be Used to Force Audit Committees to Put the Audit Out for Bids

The SEC staff has advised several companies that it will not recommend enforcement action if the company excludes from its proxy materials a shareholder proposal that would require the audit committee to periodically solicit proposals to perform the company's audit. Consistent with its longstanding view that the selection and engagement of a company's independent auditor is a matter relating to the company's ordinary business operations, the staff permitted these companies to omit a resolution submitted by Qube Investment Management Inc., a Canadian investment advisory firm, that provides: "RESOLVED - That the Board of Directors shall require that the Audit Committee will request proposals for the Audit Engagement no less than every 8 Years."

Qube reportedly submitted its shareholder proposal to 28 companies. In support of its proposal, Qube stated in its submission to the targeted companies:

"Having the audit committee issue a regular request for proposal on the audit engagement is a compromise to a forced rotation. It continues to empower the audit committee, but asks them to perform a genuine cost/benefit analysis on a potential change in auditor. The audit committee decides if a rotation brings benefit that outweighs its cost. It is our belief that competitive market forces will prevail, audit fees will reduce (or at least hold constant), while valuable governance and oversight will increase."

In a series of letters issued during January, the SEC staff advised 11 of the companies that it would not oppose exclusion of Qube's proposal. In a 1998 release discussing the shareholder proposal rule, the SEC explained that it does not require a company to include in its proxy materials shareholder proposals that impinge on ordinary business operations. The Commission explained that "certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight" and that such proposals may to an unacceptable degree seek "to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." The SEC staff has traditionally viewed proposals relating to the selection, retention, and oversight of the auditor as falling into this category and applied that approach to the Qube proposal.

Comment: PCAOB Chairman Doty's support for mandatory audit firm rotation, coupled with the European Union's decision to require rotation, are likely to mean that interest in whether audit committees should periodically change – or consider whether to change – auditors will remain active in the United States, notwithstanding the PCAOB's decision to discontinue its efforts to require rotation. Absent a fundamental change in SEC philosophy, shareholders are not however able to use shareholder proposals as a vehicle to force audit committees to change auditors or solicit tenders. The issue is more likely to be addressed through disclosure. As noted in several prior Updates (see, e.g., December 2015 Update, October-November 2015 Update, and July 2015 Update), there is considerable pressure for expanded audit

committee disclosure, either through voluntary initiatives or possible SEC rulemaking. Disclosure concerning the audit committee's reasoning regarding retention of the auditor and whether or when to consider alternatives is likely to be a more productive approach than forced rotation or proposal requests.

Auditors that Prepare the Corporate Tax Return Tend to Do So Cautiously

An academic study finds that the corporate tax returns of companies that retain their financial statement auditor to prepare the return take less aggressive tax positions than do returns prepared by either the company itself or by other kinds of external advisers. The study, "Auditors, Non-Auditors, and Internal Tax Departments in Corporate Tax Aggressiveness," was conducted by Kenneth J. Klassen, University of Waterloo, Petro Lisowsky, University of Illinois at Urbana–Champaign Norwegian Center for Taxation, and Devan Mescall, University of Saskatchewan. It is based on a review of uncertain tax positions reported under FASB Financial Interpretation No. 48 (FIN 48) by companies in the S&P 1500 during 2008-2009, coupled with information obtained from the IRS regarding the signer of the corporate return.

The full text of the study appears in the January-February 2016 issue of the American Accounting Association's publication, The Accounting Review (available here for purchase). The study's abstract states:

"Using confidential data from the Internal Revenue Service on who signs a corporation's tax return, we investigate whether the party primarily responsible for the tax compliance function of the firm—the auditor, an external non-auditor, or the internal tax department—is related to the corporation's tax aggressiveness. We report three key findings: (1) firms preparing their own tax returns or hiring a non-auditor claim more aggressive tax positions than firms using their auditor as the tax preparer; (2) auditor-provided tax services are related to tax aggressiveness even after considering tax preparer identity, which supports and extends prior research using tax fees as a proxy for tax planning; and (3) Big 4 tax preparers, in particular, are linked to less tax aggressiveness when they are the auditor than when they are not the auditor."

The authors explanation of their findings is that the auditor has more downside risk if tax positions underlying the return are rejected by the IRS than do other tax preparers, including the company's tax staff. The auditor's higher risk exposure stems from two sources: "(1) financial reporting restatement risk due to an audit failure related to the tax accounts; and (2) reputation risk, in that the auditor-preparer's work is more visible and sensitive to the firm's leadership."

As to the later point, the authors argue that audit committee pre-approval of auditor tax services, required under the Sarbanes-Oxley Act, exposes the board to potential embarrassment if the company's tax positions are rejected and that this risk incentivizes the auditor to be more cautious. "[I]f the firm employs its auditor for tax services, then its audit committee has explicitly sanctioned this relationship under the requirements of the Sarbanes-Oxley Act of 2002 (SOX). Therefore, the board of directors, as well as managers, may bear additional costs if negative tax outcomes result * * *, relative to the case if the tax work was conducted

separately from the audit." The authors also note that the PCAOB's rules prevent the financial statement auditor from advising the company to use tax strategies that have tax avoidance as a significant purpose and do not meet the standard of "at least more likely than not to be allowable." Other return preparers are not subject to this limitation.

Comment: Traditionally (i.e., since the early 2000s), non-audit services, including tax preparation, have been regarded as potential threats to auditor independence and therefore to audit quality. The theory behind this view is that the greater the aggregate fees the auditor is generating from the client, the less inclined the firm's personnel will be to risk the relationship by challenging management's views on financial reporting issues. This study looks at the issue from another perspective – promoting tax compliance – and suggests that, when viewed through that lens, auditor return preparation creates positive incentives. Of course, an audit committee considering whether to approve return preparation as a non-audit service would need to weigh a variety of factors, in addition to the auditor's potential tax conservatism, including (1) cost of the service, relative to other options; (2) the level of in-house tax expertise; (3) the value, in the company's circumstances, of having more than one perspective on the tax reserve; and (4) the risk of disagreements between the preparer and the auditor resulting in additional FIN 48 disclosures.

Cybersecurity Risk Now Tops Public Company Directors' Worries, With Reputational Risk Close Behind

Accounting firm EisnerAmper (EA) has released its sixth annual survey of directors, Concerns About Risks Confronting Boards. The results indicate that, across the public, private, and nonprofit entities EisnerAmper surveyed, directors are most worried about reputational risk, cybersecurity risk, and regulatory compliance risk. For public companies, the top areas of concern were cybersecurity/IT risk (70 percent), reputational risk (66 percent), regulatory compliance risk (64 percent), and senior management succession planning (51 percent). (No other area was cited as a top concern by more than 50 percent of public company director respondents.) These findings are largely consistent with EA's prior survey (see August 2014 Update), although concern about reputational risk has fallen somewhat this year, with the result that cybersecurity – rather than reputation – is now the most frequently-cited concern of public company respondents.

The survey included the opinions of directors serving on the boards of more than 300 publicly-traded, private, and not-for-profit organizations in a variety of industries. Half of respondents served on the board of an organization with $50 million or more in revenue, while 13 percent were from organizations with over $1 billion in revenue. Fifty-six percent of respondents indicated that they were audit committee members.

On an aggregate basis, the issues cited by respondents of all types as their top concerns (and the percentage of respondents that cited each) were:

- Reputational risk (75 percent). It is not clear how survey defined "reputational risk", although it appears to refer to an event of any

nature that threatens to injure the organization's public reputation. For example, the survey report refers to the Target Corporation cyber breach as a reputational risk event, although it would appear that the incident could also be viewed as an example of Cybersecurity/IT Risk or of Crisis Management.

- Cybersecurity/IT Risk (61 percent).
- Regulatory Compliance Risk (53 percent).
- Senior Management Succession Planning (51 percent).
- Product Risk (34 percent).
- Crisis Management (32 percent).
- Risk Due to Fraud (27 percent).
- Disaster Recovery (26 percent).
- Tax Strategies (15 percent).
- Outsourcing Risk (15 percent).
- Diversity (12 percent). AE's survey report states: "Half of the board members agreed with utilizing diversity goals; those who disagreed referenced their belief that 'experience' and 'skills' should drive board member selections as opposed to diversity factors. Not-for-profits seem to be the most progressive in incorporating limits and quotas into minimizing group think and reducing risk. Interestingly, 23% of board members ranked diversity as an important area of risk management, while only 7% for public and private as well said diversity was a main concern for their boards."

As to who is addressing risk and how well they are doing so, the following percentages of directors indicated that particular groups were performing "very well" or "well enough" with respect to risk --

- Regular board and committee meetings (92 percent).
- Risk management insurance providers (73 percent).
- External auditors (84 percent).
- Accounting department (86 percent).
- Legal and compliance group (86 percent).
- IT department (75 percent).

Respondents were also asked how helpful internal audit had been in identifying risks. Looking only at public company directors, 71 percent viewed internal audit as either "helpful" or "very helpful" in risk identification, while the remaining 29 percent saw internal audit as either "not helpful" or only "slightly helpful." As in the prior survey, private

company and not-for-profit directors gave internal audit somewhat lower grades.

In the two top risk areas – Cybersecurity and Reputational Risk – views seem somewhat mixed as to how well companies are doing in addressing the problem:

- Over 95 percent of public company respondents indicated that their company uses either internal audit or external auditors/consultants to monitor cybersecurity risk. However, only 24 percent feel their boards are well-versed in the issue.

- Forty-eight percent of board members from all types of organizations stated that their board had a plan in place to address a crisis with potential reputational risk fallout. However, only 20 percent of organizations have provided training to execute the plan. EA states that public company boards "appear to be most diligent in addressing reputational risk: almost 75% have a response plan in place and nearly a quarter have provided training."

Comment: One of the suggestions in the survey report is that boards hold an annual meeting focused on reputational risk and preparation for an event that threatens the company's reputation. EA also suggests that the board and management, with CEO involvement, formulate a plan for responding to a reputational crisis. One survey respondent is quoted as having said, "You need to have thought through the challenge and crafted potential responses beforehand so that you can react quickly. There is not sufficient time to only start developing plans once the crisis occurs."

While the various kinds of reputational risk events that may arise transcend the scope of the audit committee's responsibilities, the committee may want to consider implementing this advice within its area. This is particularly true as to cybersecurity breach issues, which, despite occasional advice to the contrary (see June 2014 Update), are often assigned to the audit committee.

Investors Don't Reward Candor About Cyber Risk – But the SEC Might

A study by three Creighton University professors concludes that company disclosures relating to cybersecurity risk are associated with significant declines in the company's share price. Reviewing the response to the SEC's 2011 guidance on disclosure regarding cybersecurity and cyber incidents, they find that few companies have chosen to make risk disclosures prior to the occurrence of a cyber breach and that those they do make disclosure suffer a decline in market price. Meanwhile, an SEC staff member has warned that companies that fail to disclose cyber breaches may face enforcement action.

In "SEC Cybersecurity Guidelines: Insights into the Utility of Risk Factor Disclosures for Investors," Edward A. Morse, Vasant Raval, John R. Wingender reviewed how companies have responded to the SEC Division of Corporation Finance's 2011 guidance entitled "Cybersecurity." The 2011 guidance states, in part, that companies "should disclose the risk of cyber incidents if these issues are among the most significant

factors that make an investment in the company speculative or risky." It directs companies to avoid boilerplate or standardized disclosures: "Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure." As to MD&A disclosure, the guidance states that "Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition." Therefore, while the guidance leaves considerable room for judgment regarding whether to make disclosure, it requires specificity if disclosure is made.

The Creighton study (which considers pre-incident risk disclosure) reaches the following conclusions:

- "Firms seem to have responded cautiously to the SEC's guidance concerning cybersecurity risks. Despite the pervasive nature of cybersecurity risks across a broad range of industries, only a small percentage of firms potentially affected by such risks have undertaken affirmative risk factor disclosures in response to the guidance. While one might expect that adding yet another item to a list of risks affecting the firm in the annual Form 10-K would not trigger an adverse reaction from the marketplace, our empirical data suggest otherwise."

- "Firms that disclosed cybersecurity risks were indeed punished by investors. This adverse market reaction suggests that caution was indeed the appropriate response from the firm's perspective. Although some firms might have concluded that disclosures might provide a favorable outcome from signaling that management was attentive to concerns in the cybersecurity environment, the investor response suggests a different signaling function was operating here."

- "* * * Those who chose not to disclose may be implying that their cybersecurity efforts are adequate to address the risks that their firms may be facing * * *. Unfortunately for those who do add cybersecurity risk factor disclosures, they may be unintentionally suggesting that they have firm-specific risk. When only some firms respond with disclosure, while others remain silent, the market appears to conclude that a disclosure suggests additional risks. The empirical data here suggest that the market is amenable to that suggestion through sending a negative impact on stock price in response to the firm's signal."

While – in the words of the Creighton authors – "Silence is indeed golden – at least from the investor's perspective", the SEC enforcement staff may have a somewhat different view, particularly as to post-cyber incident disclosure. According to an article in Law 360, SEC Deputy Enforcement Director Stephanie Avakian warned the audience at the Practicing Law Institute's February 19 "SEC Speaks" conference that the agency is concerned about situations in which companies experience breaches, but fail to make disclosure of the breach. She suggested that the Commission may bring enforcement actions in that area. "We see a spectrum of cyber awareness and attention and some firms essentially

have nothing, so this is something we have to look at." The SEC has not yet brought any cases of this type, and Ms. Avakian recognized that disclosure decisions in this area are not easy, with many variables coming into play. “We understand it may be difficult to assess the nature of a situation, these situations are fluid and core facts can change.”

Comment: The Creighton study provides an interesting insight into market psychology, but may not be a good guide for companies considering cyber risk disclosure. Ms. Avakian’s comments make clear that the enforcement staff is looking at incident disclosure. It may not be a long step for the staff, with the benefit of hindsight, to also ask whether a company that has experienced a breach gave proper pre-breach consideration to the SEC’s cybersecurity guidance. In the wake of a breach which has had clearly material consequences, the staff may want to understand whether the company had sufficient, specific ex-ante information that cyber security was a risk that company should have been disclosed, either as a risk factor or as a known uncertainty in MD&A.

Prior editions of the Audit Committee and Auditor Oversight Update are available here.

www.bakermckenzie.com

For further information please contact

www.bakermckenzie.com

Daniel L. Goelzer
+1 202 835 6191
Daniel.Goelzer@bakermckenzie.com

815 Connecticut Avenue
Washington, DC 20006-4078
United States

©2016 Baker & McKenzie. All rights reserved. Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.