November 14, 2003

VIA EMAIL

Office of the Secretary
PCAOB
1666 K Street, N.W.
Washington, DC 20006-2803

Re: PCAOB Rulemaking Docket Matter No. 8

Dear Sirs or Madams:

These comments are submitted on behalf of Guidance Software, Inc. in response to the Proposed Auditing Standard, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (the "Proposed Standard") contained in PCAOB Release No. 2003-017 (the "Release") (PCAOB Rulemaking Docket Matter No. 008). The Proposed Standard, if adopted, would be the standard on attestation engagements referred to in Section 404(b) and Section 103(a)(2)(A) of the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley").

Guidance Software applauds the PCAOB as it continues its efforts to re-establish the independence of the auditing profession and improve the quality of audits, and thus their utility to investors. The Proposed Standard, however, falls short in addressing the auditor's role in preventing, detecting, and responding to fraud. Since a lack of effective internal controls enables fraud, and the result of fraud is often an improper use or disposition of assets (and is thus covered by the definition of "internal control over financial reporting"), the audit of internal control over financial reporting should address a company's policies and practices aimed at discouraging and responding to fraud.

Although the Release sets forth thirty-one specific questions, on topics ranging from an integrated audit to auditor's independence, the PCAOB has not set forth any question concerning the issue of fraud. The entirety of the PCAOB's commentary concerning fraud, in a twenty-five-page letter, consists of one paragraph, which is set forth below:

> **Fraud Considerations in an Audit of Internal Control Over Financial Reporting**
>
> Strong internal controls provide better opportunities to detect and deter fraud. For example, many frauds resulting in financial statement restatement relied upon the ability of management to exploit weaknesses in internal control. To the extent that the internal control reporting required by Section 404 can help restore investor confidence by improving

> the effectiveness of internal controls (and reducing the incidence of fraud), the auditing standard on performing the audit of internal control over financial reporting should emphasize controls that prevent or detect errors as well as fraud. For this reason, the proposed standard specifically addresses and emphasizes the importance of controls over possible fraud and requires the auditor to test controls specifically intended to prevent or detect fraud that is reasonably likely to result in material misstatement of the financial statements.[1]

The PCAOB has glossed over the central point of Sarbanes-Oxley: that public companies must engage in effective self-policing to combat internal corporate fraud. Sarbanes-Oxley represented the Congressional response to "the shenanigans . . .that ha[d] been going on in corporate America"[2] such as the Enron debacle.[3] Thus, Sarbanes-Oxley was enacted to protect investors by combating corporate crime and improving corporate governance.[4] One of the central themes underlying Sarbanes-Oxley is that public companies need to institute and maintain adequate internal controls, which must include "controls related to the **prevention, identification and detection of fraud**."[5] (Emphasis added). As many commentators have noted, Sarbanes-Oxley requires companies to implement extensive corporate governance policies to prevent and to respond timely to fraudulent activity within the company.[6] For example, Sarbanes-Oxley expressly requires publicly traded companies to create anonymous hotlines for the reporting of fraud, it requires executives to certify that their financial statements are accurate, and it provides additional protections for employees of public companies who report fraud. The inclusion of a requirement for an internal control audit was an effort to have the auditing profession, instead of shredding evidence as in the Andersen case, directly involved in the effort to prevent, identify, and discover fraud. Clearly, the requirement that a financial statement audit encompass controls that address or mitigate fraud risk, as required by AU sec. 316, *Consideration of Fraud in Financial Statement Audit*, proved ineffective prior to Sarbanes-Oxley, at least in the eyes of Congress. Thus, a new audit requirement was instituted to have auditors conduct a separate audit of a company's internal controls.

The Section 404 requirement of effective internal controls encompasses more than mere accounting practices. In June 2003 the SEC issued its final rules under Section 404 of Sarbanes-Oxley. The SEC noted that "internal control is a broad concept that extends beyond the accounting functions of a company."[7] Under the SEC's definition of "internal control over financial reporting," a definition which the Release purportedly adopts,[8] the internal controls process must include policies and procedures that:

> Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the [company's] assets that **could have** a material effect on the financial statements.[9]

The definition is crystal clear: internal controls over financial reporting must include those controls designed to prevent or detect activities such as insider trading and other internal financial fraud, theft of intellectual property, large-scale misappropriation of customer information, or other similar losses that "could have" a material effect on the financial statements. The Proposed Standard, however, narrows the "safeguarding of assets" function of internal controls to "protection only against losses arising from intentional and unintentional misstatements in processing transactions and handling the related assets."[10] As noted above, however, safeguarding of assets is intimately linked to the prevention and detection of fraud; the occurrence of fraud often leads directly to the misappropriation or destruction of a company's assets. Note that the COSO Framework recognizes that one of the "temptations" for employee fraud is "nonexistent or ineffective controls," as well as "high decentralization that . . . reduces the chances of getting caught."[11] Thus, in order to prevent employee fraud, or unauthorized acquisition, use or disposition of a company's assets, the company should have in place effective controls that increase the likelihood of getting caught. In discussing fraud, however, the Proposed Standard restricts the review of controls "intended to address the risks of fraud that are **reasonably likely** to have a material affect on the company's financial statements."[12] As a result, a failure of controls against fraud that "could have," but is not "reasonably likely to have," a material affect on the company's financial statements is written out of the Proposed Standard. There is no justification for this narrow focus. Rather, the Proposed Standard should focus on controls to fight fraud (which leads to unauthorized acquisition, use or disposition of the company's assets) that **could have** a material effect on the financial statements.

A pair of hypotheticals highlights the shortcomings of the Proposed Standard:

> 1) Assume a company in which a senior executive who has access to material, nonpublic information is facilitating a friend's trading in the company's stock based on that information, in violation of the company's internal policies and the securities laws, by using an instant messaging service. Assume further that the company has failed to implement available technology that would allow it to capture the relevant evidence concerning the rogue employee's activities, and thereby enforce its policies, and refer the case to law enforcement.[13] Finally, assume that public knowledge of this executive's activities would materially harm the company by causing it to defend itself from regulatory investigations and shareholder suits. In an audit under the Proposed Standard, the Company's "nonexistent or ineffective controls," to use the COSO language, would be unlikely to be unmasked, since the controls in question would not govern "intentional and unintentional misstatements in processing transactions." Certainly, if the auditors uncovered the executive's fraud, it would result in at least a significant deficiency under Section 126 of the Proposed Standard. However, the auditing profession's track record in uncovering executive fraud is not comforting. It would be far better for auditors to focus on looking for and demanding effective controls that increase the

likelihood of catching employee malfeasance, thereby helping prevent employee fraud in the first place.

2) Assume an entertainment company that has valuable intellectual property, both in already released films, and in films currently being produced. Assume further that if one of the pre-released films were to transmitted by a rogue employee to a file-sharing website prior to the scheduled launch of the film, that the company would suffer material financial harm. Finally, assume that the company has failed to install readily available controls to detect the rogue employee's unauthorized disposition of this important company asset. Under the definition of "internal control over financial reporting," the hypothetical entertainment company has a problem (whether defined as an internal control deficiency, a significant deficiency, or a material weakness) – its internal controls do not "provide reasonable assurance regarding prevention or timely detection of unauthorized . . . disposition of . . . assets that could have a material effect on the financial statements." Under the Proposed Standard, however, the auditors would have nothing to say about this hypothetical company's grievous lack of internal controls, because the controls in question would not govern "intentional and unintentional misstatements in processing transactions."

COSO specifically recognizes the risks of internal wrongdoing: "Former or disgruntled employees can be more of a threat to a system than hackers."[14] Indeed, "the assessment of risks not only influences the control activities, but may also highlight a need to reconsider information and communication needs."[15] The Proposed Standard does nod towards the broader COSO approach by noting that "[t]he auditor should identify all controls that could materially affect financial reporting, including controls that focus primarily on the effectiveness and efficiency of operations or compliance with laws and regulations and which also have a material effect on the reliability of financial reporting."[16] The Proposed Standard, however, should focus more on those controls that can safeguard the company's assets from fraud or other unauthorized use or disposition. For example, Section 126 of the Proposed Standard sets forth specific circumstances that "should be regarded as at least a significant deficiency and [are] a strong indicator that a material weakness in internal control over financial reporting exists."[17] In addition to the items listed, there should be added:

- Fraud prevention, detection and/or response programs and controls are ineffective.[18]
- Controls to protect the company's assets from unauthorized acquisition, use or disposition are ineffective.

As noted above, Section 126 of the Proposed Standard lists "[i]dentification of fraud of any magnitude on the part of senior management." Certainly, if fraud is identified, that is indicative

of a serious control issue. The more fundamental point, however, is that the lack of effective controls to prevent, detect, and respond to fraud is a serious control issue, whether or not any fraud is identified at the time of the audit. Moreover, it is a control issue that ultimately impacts the accuracy and quality of the company's financial reporting.

In sum, internal fraud and insider malfeasance in corporate America caused widespread harm to investors and the overall economy, leading directly to the passage of Sarbanes-Oxley. Because the lack of adequate controls to deter, prevent, and respond to such fraud creates an unreasonable risk of such fraud occurring, which very well could impact the financial statements, the standard ultimately adopted by the PCAOB should, at a minimum, require auditors to address a company's internal controls for fighting fraud.

Sincerely,

Guidance Software, Inc. by:

/s/ Victor T. Limongelli

Victor T. Limongelli
General Counsel

---

[1] Release, at 20-21.
[2] Representative Bentsen, 148 Cong. Rec. H5462-02, at *H5467.
[3] Congress acted "in response to Enron, Global Crossing and other bankruptcies." Representative Oxley, 148 Cong. Rec. H5462-02, at *H5462. *See also* "The events of the past months have underscored the importance of transparency in corporate governance. While many believed that Enron was an isolated occurrence, the failures of Tyco, Global Crossing, and WorldCom have eroded confidence in the markets, both here and overseas" Representative Jones, 148 Cong. Rec. H5462-02, at *H5469.
[4] According to Senator Sarbanes, "[t]he bill sets significantly higher standards for corporate responsibility governance. . . . There are also extensive criminal penalties contained in this legislation . . . These provisions, among other things, require the CEOs and CFOs to certify their company's financial statements under penalty of potentially severe punishments." Senator Sarbanes, 148 Cong. Rec. S7350-04, at *S7351.
[5] 68 FR 36636, 36643, June 18, 2003.
[6] Another galvanizing factor was the rampant destruction of computer evidence that occurred in the Arthur Andersen/Enron case. *See* the Arthur Andersen indictment, which alleges that "an unparalleled initiative was undertaken to . . . delete computer files" available at:
http://news.findlaw.com/hdocs/docs/enron/usandersen030702ind.pdf
[7] 68 FR 36636, 36638, June 18, 2003.
[8] Release, § 6.
[9] 68 FR 36636, 36640, June 18, 2003 (Emphasis added).
[10] Release, Appendix C, ¶ C1.
[11] COSO Framework, at 25.
[12] Release, § 24.

[13] Even before the passage of Sarbanes-Oxley, the SEC's official position regarding internal investigations was that effective self-policing and cooperation with law enforcement could reduce or even eliminate a corporation's liability for violation of the federal securities laws. For instance, the SEC's investigation into Seaboard Corporation found that the controller of one of Seaboard's divisions had caused Seaboard's books and records to overstate assets and understate expenses, and had subsequently actively concealed such misstatements. *See In the Matter of Gisela de Leon-Meredith*, Exchange Act Release No. 44970 (October 23, 2001). Although the SEC ordered relief against the controller, it took no enforcement action against Seaboard, due to the company's prompt and thorough response to the incident, as well as its cooperation with the SEC. *See* Exchange Act Release No. 44969 (October 23, 2001). The SEC noted that the public at large benefits when "businesses seek out, self-report and rectify illegal conduct." Id. The SEC, in deciding "whether, and how much, to credit self-policing, self-reporting, remediation and cooperation," (Exchange Act Release No. 44969 (October 23, 2001)) established four broad measures for it to assess:

- Self-policing prior to the discovery of the misconduct . . .
- Self-reporting of misconduct when it is discovered, including conducting a thorough review of the nature, extent, origins and consequences of the misconduct . . .
- Remediation . . . modifying and improving internal controls . . .
- Cooperation with law enforcement authorities, including providing the [SEC] staff with all information relevant to the underlying violations . . .

SEC Release 2001-117 (October 23, 2001). Indeed, in order to cooperate effectively with the SEC and law enforcement, a company must be able to "identify . . . evidence with sufficient precision to facilitate prompt enforcement actions against those who violated the law." Exchange Act Release No. 44969 (October 23, 2001).

[14] COSO Framework, at 53.

[15] COSO Framework, at 18.

[16] Release, § 14.

[17] Release § 126.

[18] Although Section 123 of the Release mentions "antifraud programs and controls," it does so in the context of discussing the interaction of qualitative and quantitative considerations. It would be better addressed in Section 126.