March 31, 2005

Mr. Jonathan G. Katz, Secretary
Securities and Exchange Commission
450 Fifth Street N.W.
Washington, DC 20549-0609

Re: File # 4-497

Dear Mr. Katz:

Response to request for feedback on SOX Section 404

Taxware LP is pleased that the Securities and Exchange Commission ("SEC") is soliciting feedback on the implementation of the internal control requirements under section 404 of the Sarbanes-Oxley Act of 2002 ("the Act"). Taxware LP is a leading provider of global transaction tax compliance software to Fortune 1000 companies.

Our client base has material exposure to transaction taxes globally. In numerous jurisdictions Value Added Tax ("VAT") obligations represent 25% of gross sales. Although rates tend to be lower, there are 7,588 discrete retail sales tax ("RST") jurisdictions in the US, making domestic compliance complex and burdensome. These obligations place our clients under considerable pressure to accurately determine, collect, and remit the correct tax around the world, every minute of the day. Inaccurate computations can weaken commercial competitiveness, violate local laws, and contravene governance regulation. Good governance and effective compliance are not possible in this context without secure automated systems.

It is our experience that not only in our area of expertise (taxation), but in most other areas of corporate governance, it is not possible for an international company to comply with regulatory standards without comprehensive technological controls over the information systems within the firm. The Act therefore, without stating so directly, relies fundamentally on information security. The core provisions of the Act, Sections 302 and 404, raise the issue of information security most directly.

Section 302 requires that a public company's principal executive officer and principal financial officer certify the accuracy and fairness of the company's periodic reports. Section 302 requires these same officers to certify (a) that they are responsible for establishing and maintaining the internal controls, (b) that they have disclosed to their auditors and/or audit committees any significant deficiencies in the design and operation of the internal controls, and (c) that they have disclosed in required periodic reports any significant changes in the internal controls that might affect those controls subsequent to the date of their evaluations. Accurate and timely disclosures are not possible without robust and secure technology systems.

Section 404 also implicates information security practice and procedure. Section 404 mandates that the annual report filed by a public company contain an "internal control report" which: (a) states the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (b) contains an assessment, as of the most recent fiscal year of the company, of the effectiveness of the internal control structure and procedures for financial reporting. Once again, the Act necessarily requires that firms possess effective information security to accomplish their mandate.

These provisions of the Act function in tandem with Auditing Standard Number 2 of the Public Company Accounting Oversight Board ("PCAOB") *An Audit of Internal Control over Financial Reporting Performed in conjunction with an Audit of Financial Statements* ("AS No. 2"). Together these statutory provisions and rulings have increased the evaluative rigor exercised over corporate cash flows. It seems apparent, however, that these requirements may have gone a bit too far in their rigor and may have missed their more appropriate focus.

In AS No. 2 the PCAOB takes the position that the auditor must conduct a formal audit of the internal controls and then issue an audit opinion on the internal control structure of the company. This activity, while commendable from a theoretical point of view, has resulted in a considerable increase in audit fees without a correspondingly significant increase in shareholder value and investor confidence. The reason for the lack of benefit is that the required activities constitute labor-intensive reviews of routine processes that are unnecessarily duplicative.

Three reports are required under the present rules: (a) the management assessment report, (b) the opinion on management's assessment, and (c) the opinion on internal control. While it is critical that management assess the effectiveness of the company's internal controls [item (a) above], and it is equally essential that the auditor issue an opinion on the effectiveness of the system of internal controls [item (c) above], it is not essential for the auditor to conduct a formal audit of the process that management uses to arrive at its assessment [item (b) above].

There is an alternative approach, one that would give the SEC and investors the assurances they need in assessing the efficacy of internal controls; one that would allow the PCAOB to modify the AS No. 2 standard to one of attestation rather than audit.

We advocate an approach that emphasizes technology and information security, and thereby minimizes the need for traditional audit and audit opinions when assessing management's report. The essence of sections 302 and 404 is that entities covered by the Act must have a reasonable and appropriate information security policy, one that is designed to assure the integrity of their internal controls and procedures for financial reporting. It is this security regime, once realized and implemented by management that is the critical element in improving the reliability of company data. It is this reliability, in turn, that will improve financial reporting, and will assist the public to regain confidence in corporate governance.

The drive for increased reliability in the processing and recording of financial transactions is something we see regularly in our specialty field of transaction taxes. The most

notable development in this regard is contained in the Streamlined Sales Tax Initiative (SSTI), an industry-government agreement that Taxware LP has strongly advocated since its inception over five years ago.

The SSTI is an agreement among the US states to simplify the tax collection process. One of the most innovative aspects of the SSTI is the certification of tax collection software used by vendors. The proper use of this software by companies essentially indemnifies vendors from liability for errors in determining the appropriate tax due to participating jurisdictions. The vendor is no longer subject to state "audits" (barring fraud), although it is subject to "system checks" by state authorities to make sure that the system is functioning properly. The reason for the indemnification is that the regulators (in this instance the state revenue authorities) know in advance that the software is accurate and effective, that the correct taxes have been imposed, the funds remitted to the correct jurisdictions, and that factually accurate and timely returns have been filed.

It should be clear that, in an SSTI scenario, not only is the risk of corporate transaction tax liability reduced (or eliminated), but that audit oversight is independently buttressed. The statutory auditor can, and should, appropriately pull back. The auditor (like the state itself) can be primarily concerned with the human intervention component in the financial system. Such an oversight regime is more akin to an attestation standard than an audit standard.

In this regard Taxware LP has become the leader in developing Sarbanes-Oxley compliant, SSTI certifiable, fully automated tools for global transaction tax compliance. It is Taxware LP's experience that there are many more "certifiable" software applications in the marketplace, ones that cover other critical, but routine aspects of corporate governance. It is our suggestion that software certification may be a direction in which the SEC and PCAOB might consider looking in the effort to increase the reliability of financial reports while decreasing corporate audit costs.

Sincerely,

Richard T. Ainsworth
Tax Counsel