Sent: March 17, 2006

To: Mr. William Gradison, Acting Chairman
Public Company Accounting Oversight Board

From: Jeff Barber - Accu-Rate Telecom, El Paso, Texas, accuraterefund@earthlink.net

Subject: File NO. 4-511, Internal Control Roundtable (Sarbanes-Oxley Section 404)

Background: I have spent 15 years as an auditor, assisting clients with cost containment. For the last five years, I have served as Vice President of a hospital bill auditing practice. My team has not seen a single correct employee benefit hospital bill in over two and a half years.

By implementing SOX-compliant internal controls for healthcare expenses; a corporation can generate significant returns for shareholders and savings for employees**.** Ironically, this category has received little attention from internal auditors, CFOs, CPAs, and Audit Committees. I know of a case in which a company was deemed “compliant” by a highly respected CPA. An audit revealed that the firm’s contracted TPA had paid over $2.4 million in healthcare expenses that were not owed by my client. This amounted to an overpayment of $2,400 for every employee, during a one-year period.

Comments:

A gap in internal controls is causing US corporations to lose billions of dollars in shareholder equity and forcing current and retired employees to pay excessive healthcare charges. This accounting deficiency is found in every segment of every industry and is leading to widespread violation of SOX SEC 302, SOX 404, and ERISA SEC 1109.

The Problem: Excessive Charges in Hospital Bills

- According to a report by the National White Collar Crime Center (October 2005); based on GAO estimates, healthcare fraud amounts to approximately $170 billion per year. This does not refer to lost shareholder value, but rather to actual hard dollars that are being thrown away.

- Estimates (confirmed by an Equifax study) are that over 90% of hospital bills contain errors—most of which are overcharges, in the hospitals’ favor.

- According to a CMS study of 160,000 Medicare hospital bills; the average bill contains overcharges ranging from 5.6% in some states to over 26% in others. (We have found the percentage of overcharges to be even higher in bills submitted to corporate health plans than in those submitted to the Medicare program.)

The Gap in the System: Lack of Internal Controls for Healthcare Accounting

Self-Insurance: Approximately 1,600 publicly traded US corporations “self-insure” or “self fund” for employee benefit healthcare. Rather than purchasing indemnity health insurance or an HMO, a self-insured firm establishes a trust for the payment of employee healthcare expenses.

Most self-insured health plans retain the services of a Third Party Administrator (TPA) to verify eligibility and pay claims. In essence, the TPA is an external Accounts Payable Department for healthcare. In order to comply with privacy issues legislated under HIPAA; the TPA operates with little or no oversight by the corporation’s internal auditors or outside CPA.

There is a common misconception (even among Audit Committee members) that TPAs verify the accuracy and validity of employee healthcare bills, prior to paying claims. In actuality, TPAs and Preferred Provider Networks do not have the time, resources, expertise, or contractual obligation to confirm the accuracy of specific line-item charges.

Most TPAs pay employees' hospital expenses from summary bills ("UB-92s"), which provide no itemization of charges. These simple invoices list charges by department only (Operating Room, Radiology, etc.), much like the first few pages of a phone bill. The difference? A phone bill provides several pages of detail, indicating every single call that is incorporated into the "balance due." Unfortunately, no such detail exists on a UB-92.

Example: A hospital might charge a self-funded corporation $38,329.50 for medications described only as "Drugs-Generic." The summary bill would not specify the names of the medications, the quantities provided, or the unit pricing. Under the current system, it is impossible to verify the accuracy of employee benefit hospital bills. As a result, publicly traded corporate health plans routinely pay for:

a) Hospital services that have not been provided;
b) Hospital services that have been charged at an inflated rate.

Separate Accounting Standards

Suppose a corporation received an invoice that included a $12,000 charge for "Office Supplies," with no description of the products. The Accounts Payable Department would request additional information, before issuing payment.

If the corporation's TPA received a summary invoice that included a $12,000 charge for "Operating Room Services," the TPA would routinely write a check for that bill, and for every other medical claim that arrived that week. The TPA would then send the firm a recap of total funds expended on its behalf for the week, often in the form of a "summary of summaries;" e.g., "Physician Office Visits: $25,686; Hospital Charges: $182,943; Pharmacy Charges: $31,884." Such practices represent a duality of standards, inconsistent with the intent of SOX 404.

Unknown Pricing

Many corporate health plans have a record of the discount rate that has been negotiated with hospitals (e.g., 20%), but no record of the base prices that are to be used in the calculation of discounts. In fact, many TPAs claim that hospital prices are "confidential." When TPAs do not make that claim and attempt to acquire pricing from Preferred Provider Networks; they usually find that the Networks deem the prices "proprietary" and claim that corporate clients have no right to see the billing detail.

In order to verify the accuracy of hospital bill charges, corporations must have a standard pricing schedule (e.g., the "Usual, Customary and Routine" rate or "UCR"). Providers' discounts are applied to these prices.

If a hospital wishes to treat Medicare and Medicaid patients, it is required to file its prices with the Federal Government. If pricing standards are not established, a hospital may inflate its prices by as much as 500%, before applying the negotiated discounts.

In a publicly traded corporation, if no one knows what the prices should be; any certification of the adequacy of internal controls is misleading. In a worst case scenario, such certifications could be fraudulent.

Inconsistent Pricing

In Houston, Texas, the cost of an aspirin in an inpatient Pharmacy may be 2 cents in one facility and $35.72 in another. The variance is almost 1,800%. This would be equivalent to a gas station charging $4,018.50 per gallon for gasoline, in a market in which gas was available for $2.25.

An internal control system is inadequate if it (a) allows a 1,000% variation in pricing for a given product or service; or (b) allows a health plan to pay 1,000% more than the retail market price for products or services.

Invalid Charges

Some subcontracted health plan administrators fail to confirm eligibility, prior to issuing payment. As a result, some self-insured corporations are paying hospital expenses for individuals who are not covered by the corporate health plan. For example, in a three-year period, one TPA paid the healthcare expenses for 210 individuals who were <u>not associated with the employer.</u>

An internal control system is inadequate if it allows a corporate health plan to pay the expenses of people who are not associated with the corporation.

"No Audit" Provision

In spite of the fact that most TPAs are not contractually obligated to verify the accuracy of their clients' hospital bills; many TPA agreements have a "no audit" provision, which prevents the <u>client</u> from reviewing the accuracy of the TPA's accounting. By agreeing to a "no audit" provision, a corporation essentially allows the TPA to have unfettered access to the corporate checkbook. If a TPA contract does <u>not</u> have a "no audit" provision, it probably contains a "hold harmless" clause, which prevents the TPA from being held accountable for overpayments. This leaves the client without recourse to the TPA and forces the corporation to seek restitution from the Network.

If a corporation has agreed to a "no audit" provision, it cannot certify the adequacy of internal controls.

Accounting Firms

Many corporations rely on subcontracted accounting firms to verify the accuracy of employees' hospital bills. In reality, accountants generally review the mathematical calculations (e.g., the sum of the billed charges and the application of negotiated discounts) in a sampling of hospital bills. Given that such bills are in summary format, without itemization; billing errors remain undetected. As a result, CEOs and CFOs are certifying financial documents that are based, in part, on inaccurate information.

Additionally, corporations are relying on their accounting firms' assertions that SAS70 Type 2 audits are protecting them from personal financial and criminal liability. This could not be further from the truth! Authority to audit can be delegated; but responsibility and liability for internal control deficiencies *cannot* be delegated.

Privacy Issues

As a result of HIPAA privacy requirements, employers are in a difficult position. Although internal auditors are not permitted to review employees' hospital bills, corporations are required to certify the accuracy of financial reports.

Audit Committees

Audit Committees have the responsibility of establishing "procedures for the receipt, retention, and treatment of complaints received by the issuer regarding…internal accounting controls…"

We have encountered a lack of "corporate governance compliance" relative to internal controls. Specifically, we are aware of corporate employees intercepting Certified Mail (pertaining to internal control deficiencies), which has been sent to Audit Committee members.

In a few cases, we have sent information to an Audit Committee member at his/her business or home address. We know of a case in which an Audit Committee Chairman has refused to accept delivery of an envelope marked "Sarbanes-Oxley."

Many Audit Committee members earn in excess of $400 per hour for their services. When an Audit Committee member refuses to accept mail that pertains to an internal control issue; he/she is not performing his/her fiduciary duties, as required by Sarbanes-Oxley.

In many corporations, the Chief Legal Officer also serves as the Corporate Secretary. When a CLO prevents Audit Committee members from receiving information pertaining to internal control deficiencies; his/her actions cause the CEO and CFO to file false and misleading internal control certifications to the SEC and shareholders.

"Double Dipping" by Consultants

Many corporations are unaware of fees and commissions that their consultants are receiving from other entities.

For example, an employee benefits consultant, receiving $200 per hour from the corporation, may also be receiving compensation from a healthcare provider. (We have seen a case in which a consultant has received an undisclosed "honorarium" of $180,000 per year for a single account.) Such business relationships represent a conflict of interest.

Internal controls are inadequate if a corporation's consultant is accepting undisclosed payments from an entity that is <u>overcharging</u> the corporation.

Corporate Indifference

Many corporate officers and Audit Committee members believe they are immune from SEC prosecution relative to internal control deficiencies. Although most CEOs and CFOs are aware of excessive charges in hospital bills, they seem confident that (a) their TPAs are correcting the errors and (b) the SEC is not interested in internal control issues that result in overpayments to hospitals--regardless of the cost to corporations, employees, and shareholders.

Impact on Shareholder Value

We recently reviewed a hospital bill for an employee of a publicly traded firm. The bill contained over $40,000 in overcharges. In spite of the fact that the firm's internal controls had overlooked a $40,000 error in a single invoice, the Audit Committee Chairman, CEO, and CFO failed to act. As a point of reference, the firm was trading at approximately 10 times earnings. The correction of this single overpayment would have represented $25,200 in additional net, after-tax earnings and $252,000 in additional shareholder value.

Materiality

Healthcare benefits constitute a significant expense for every publicly traded firm in America. In many cases, hospital overcharges amount to $300-$400 per employee per year. (These figures represent the total overcharges divided by the <u>total</u> number employees--including employees who have not been hospitalized). If internal controls are grossly deficient and/or health plan members incur higher-than-average healthcare expenses, the cost to the corporation may rise to $1,000 or more per employee per year. Clearly, such expenses are damaging to employees, retirees, and shareholders. **In some corporations, full compliance with SOX Section 404, regarding health benefit accounting, will increase earnings per share by 2%-4%**

Recommendations:

1. SEC onsite audit personnel should review the Health Benefit Audit Plan as a part of their standard operating procedures.

2. SEC onsite audit personnel should review Health Benefit Exception Reports as a part of their standard operating procedures.

3. SEC should investigate corporate officers who conceal their firms' internal control deficiencies from Audit Committee members.

4. SEC should investigate Audit Committee members who fail to act, when advised of potential internal control deficiencies in the firms they represent.

5. Corporate Internal Audit personnel should include Health Benefits Auditing in their annual Audit Plan; and should report their findings (i.e., health benefit overcharges and fraud) to the Audit Committee on a quarterly basis.

6. Corporate Internal Audit personnel should conduct an annual Eligibility Audit and report their findings to the Audit Committee. The report should include a certification that all health benefit payments were made on behalf of employees, retirees, or dependents who were eligible to participate in the plan.

7. Corporate Internal Audit personnel should seek refunds for all payments inadvertently made on behalf of individuals who were (a) <u>not</u> associated with the corporation or (b) <u>not</u> eligible to participate in the plan (e.g., adult children who had passed the age limit for dependents). Results should be reported to the Audit Committee.

8. Corporate Internal Audit personnel should prepare an annual Commission Disclosure Document, stating all commissions, fees, and honoraria paid to TPAs, insurance brokers, consultants, Preferred Provider Networks, and hospitals. Such Disclosure Document should be reported to the Audit Committee.

9. Internal Control Consultants and Employee Benefit Consultants (retained by publicly traded corporations) should be required to provide a notarized affidavit indicating any additional compensation they are receiving from third parties; e.g., TPAs, Stop Loss Carriers, Preferred Provider Networks, hospitals, and brokers.

10. Corporate Internal Audit and Loss Prevention personnel should work in cooperation with the FBI Health Fraud Task Force and the US Attorney's Office, to facilitate the filing of criminal charges against healthcare providers, TPAs, Preferred Provider Networks, and/or insurance brokers that have defrauded publicly traded corporations.

11. Corporate personnel assigned to conduct audits should be required to have an accounting background (e.g., a minimum of 6-9 semester hours of accounting coursework), as deemed appropriate by PCAOB.

12. Internal control deficiencies should be disclosed to shareholders in the appropriate SEC 10K or 10Q within 90 days of the discovery of the deficiency.

13. It should be a violation of Section 404 for any corporate officer to certify the adequacy of internal controls, if the corporation has entered into an outsourced payer's contract that includes a "no audit" provision.

14. It should be a violation of Section 404 for any corporate officer to certify the adequacy of a firm's internal controls, unless the firm has baseline healthcare pricing data on file.

15. It should be a violation of Section 404 for any publicly traded corporate officer to certify the adequacy of internal controls if the firm outsources Sarbanes-Oxley internal control compliance to any consultant or insurance broker who is accepting payments from a TPA, Stop Loss Carrier, Preferred Provider Network, hospital, or any other health-related entity that would represent a conflict of interest.

16. Any health benefit and/or hospital bill auditing practice retained by a publicly traded corporation should be required to disclose, in writing, any relationships with and/or any compensation received from a TPA, Stop Loss Carrier, Preferred Provider Network, hospital, or any other health-related entity that would represent a conflict of interest.

17. The SEC should address the fact that corporations rely on the SAS70 Type 2 audit of external accounting firms. By relying on such audits, a corporation is NOT meeting its requirements under ERISA (the "Prudent Man Standard," among others) or any requirements under SOX 404.

18. All corporations provided <u>any</u> variance in adherence to any of the aforementioned suggested requirements should be required to publicly disclose, in their quarterly filing, the basis for all variances, the granting agency, and the basis of the authority for that variance. They should also be required to disclose the additional amount of time that the granting authority has allowed, in order for the corporation to be compliant.

19. All public corporations should be required to carry ERISA/SOX liability insurance to indemnify the owners of the corporation (the shareholders), in the event that a fiduciary breach would result in a loss in stock value, which the corporation would have to correct out of current (or future) income.

20. All individuals within the entire chain of command--from the HR contact person working directly with the Consultant, TPA, or Network to the Chairman of the Audit Committee--should be held directly accountable for ALL fiduciary breaches. A defense of "No Direct Knowledge," "No Direct Involvement," "No Direct Control," etc. should <u>not</u> be permitted. Fiduciary liability should be "strict liability," as it is of significant societal impact when a breach occurs.