University of Mississippi

eGrove

Newsletters

American Institute of Certified Public Accountants (AICPA) Historical Collection

2008

Focus, vol. 4 no. 2, March/April 2008

American Institute of Certified Public Accountants. Business Valuation and Forensic & Litigation Services Section

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_news

Part of the Accounting Commons, and the Taxation Commons

FOCUS

March/April 2008
Vol. 4, No. 2

Newsletter of the AICPA
Forensic & Valuation Services Section

What's Inside

2 A risk for CEOs and other business leaders offers CPAs an opportunity to provide services.

3 The author of the lead article follows up his fraud story with some guidance on using computer-assisted forensic techniques.

4 Recent incidents involving product quality and recalls have prompted companies to address the issue of extending compliance and ethics standards to third parties with whom they're involved.

6 An overview of the 2007 AICPA National Business Valuation Conference

7 FYI . . . Does fraud speak for itself?
> AAA proposes forensic section

Letters to the Editor

Focus encourages its readers to write letters on forensic and valuation services issues and on published articles. Please remember to include your name and telephone and fax numbers. Send your letters by e-mail to wmoran@aicpa.org.

A Life in Crime: Part I—The Smoking Gun

By William C. Barrett III CPA/ABV, CVA, CTP, CCFM

The following article is adapted from "Forensic Accounting for Business Entities," a CPE course written by William C. Barrett III for Thomson Tax & Accounting.

It was an internal coup.

The company was positioned to make an initial public offering (IPO). The product offering was a patient appointment concierge service that worked with group medical practices throughout several southeastern states. The service had been tested and refined over several years and was now ready, with deep-pocket backing, to make its debut in an IPO.

However, two of the corporate officers, both doctors and both board members, as well as the deepest pocketed of the deep-pocket investors, initiated action to remove the operating and finance officers and their staffs just prior to the offering. The deep pocket investor was withholding funds until they were terminated and replaced by his and the other officers'/board members' choices.

The attorney for the CEO and CFO had no proof that the three were conspiring and needed evidence that they were. We were asked to analyze the hard drives of the company's server and the two laptops the company provided the two doctor board members. Our mission was to search for data that might show the court that an illegal coup was being staged. The two doctors had been barred from entering the company's premises. The order had been issued after they had left work one day, and both had left their laptops on their desks. The laptops were kept in the company safe—now with a new combination code.

We conducted a forensic examination of their offices and then the company's server, but to no avail. After investigating files on the laptops' hard drives, we found nothing we could use. We were at an impasse.

But breaks sometimes come. We uncovered that the conspirators did communicate through e-mail—not the company's Outlook e-mail running through the server—but on outside sites where they had accounts with Yahoo! and Hotmail. Now we had something.

Examining External Evidence

We performed a mirror image of the second laptop's hard drive. The CEO had narrowed down to a three-day period when the two doctors started to voice, in unison, how and why the CEO, CFO, and their staffs were to be terminated because the investor "had lost confidence in them" and was withdrawing his critical financial support until they were replaced before the IPO.

The investor lived in a rural paradise more than 100 miles away from the company headquarters. We checked the company's telephone records and the doctors' company cell phone records for this time period. There were no calls with the investor on the company phones, but there were increased

Continued on page 2

Continued from page 1

conversations among the three during this time period on the doctors' cell phones, with a few calls directly before and afterward.

Looking for Ghosts

Now we had something to go on. We began to look for ghosts (a *ghost* is a writing to the hard drive that remains cached in Random Access Memory or RAM).

When you think about it, it seems quite logical. When you write an e-mail on your computer from an Internet e-mail account, what is really happening? That message isn't held in virtual space; it is written to your hard drive. But because it is not saved to your hard drive, the metadata—the tags (also written to the hard drive) that tell your computer what you are doing and where on your computer it is being done—are deleted from the tracking file when you turn the computer off. However, a ghost of the tags remains, even though they may be overwritten by new data.

Forensic software is pretty comprehensive these days. We knew that during this three-day time period, there was no reason for any correspondence to take place on the doctors' laptops with the investor's name attached to it. So we queried the software to find if the investor's name had been written to the hard drive during this time period and, if so, to track the metadata attached to the investor's name to the whole writing.

Bingo! You guessed it—we got the smoking gun: correspondence between the investor and the doctors that laid out the whole process and the doctors' roles in staging the coup. We even got their admittance that care was needed because what they were attempting was illegal.

Who could ask for anything more?

With the coup blocked, the doctors and an investor thrown off the board, and new investors waiting in the wings, the IPO went forward.

Lessons Learned

Nothing really disappears. It may be destroyed, but if it isn't destroyed properly, it is still there and can be found. (See "Computer-Assisted Forensic Techniques" on page 3.)

I have also learned that there will always be enough fraud and corporate corruption to keep me busy and happy. Sometimes I don't even get under the covers when I go to sleep because I don't want anything getting in the way when I jump out of bed, raring to go in this wonderful brand new day that is pulling me into some exciting and challenging adventure.

Also, there will always be enough need for fraud detection to go around—so get out there! Incorporate forensic accounting into your career. You will help the profession of public accounting to continue to be a shining beacon of respect and trust.

WILLIAM C. BARRETT III, CPA/ABV, CVA, CTP, CCFM, a sole practitioner in Richmond, VA, has investigated fraud and misfeasance in corporations, boards of directors, and medical practices and has directed teams investigating multidefendant money laundering, illegal income, tax evasion, and white-collar fraud. Bill sits on the Ethics Oversight Board of the National Association of Certified Valuation Analysts (NACVA) and is a member of the Virginia Society of CPAs Editorial Task Force. Contact him at billbarrett@barrettpc.com.

Lack of Ownership of ESI Policies

A severe risk for business leaders may offer an opportunity for CPAs to provide services.

CEOs and other business leaders are likely to be at business risk when their organizations lack policies on handling electronically stored information (ESI), even if they are rarely involved in developing or enforcing that ESI policy. This is the key finding in a new independent study commissioned by Kroll Ontrack®, a provider of paper and electronic discovery services as well as computer forensics and courtroom and presentation services.

Canvasse Opinion conducted the survey, interviewing in-house counsel in commercial businesses. The results suggest that helpful guidance is needed by CEOs and in-house counsel in dealing with the issues associated with ESI storage and maintenance policies, as well as discovery of ESI. This guidance could be provided by CPAs who are knowledgeable about and experienced in this area.

Continued on next page

FOCUS,
March/April 2008, Volume 4, Number 2. Published by the American Institute of Certified Public Accountants. Copyright © 2008, by the American Institute of Certified Public Accountants, Inc. 1211 Avenue of the Americas, New York, NY 10036-8775. Printed in the U.S.A.

Editorial Advisers

Travis Chamberlain, CPA/ABV, ASA
Clifton Gunderson LLP
Indianapolis, IN

Bryan Lester Coffey, CPA
Coffey Communications, LLC
Bethesda, Maryland

Jeffrey K. Mock, CPA/ABV
CPA Consulting, Inc., P.S.
Bellevue, Washington

Michael D. Rosen, CPA/ABV, PhD
Schulze Haynes Loevenguth & Co., LLC
Los Angeles, CA

Ronald L. Seigneur, CPA/ABV, CVA
Seigneur Gustafson Knight LLP
Lakewood, Colorado

Rob Shaff
Colton Consulting
Oklahoma City, Oklahoma

Holly Sharp, CPA, CFE, CFP
Laporte, Sehrt, Romig & Hand
Metairie, Louisiana

Judith A. Wagner, CPA/ABV, CVA
Wagner Valuation & Financial Forensics, LLC
Albuquerque, NM

Editor

William Moran
wmoran@aicpa.org

Responsibility and Accountability

Fewer than half of organizations (43% in the United States, 48% in the United Kingdom) have a strategy or policy in place on how to deal with ESI in litigation or internal investigations. In the United States, 41% of respondents said their in-house legal departments are responsible for developing that policy. However, almost one-fifth of respondents (19%) said the CEO should be held accountable if that policy results in government fines, court-imposed sanctions, or damage to reputation.

"These statistics are alarming but not surprising. The explosion of electronic information and the onslaught of new rules, regulations, and laws have made it incredibly difficult for companies and counsel in the United States and the United Kingdom to keep up," said Kristin Nimsger, president of Kroll Ontrack. "There is no clear definition of who should be developing or enforcing ESI policies, which precipitates a lack of ownership. However, with the size of fines and severity of sanctions possible, this issue has moved from an IT or legal issue to a threatening business issue, for which today's executives and boards need to be involved."

Getting Up to Speed

Kroll Ontrack's research also shows that, in the United States, only 25% of in-house counsel say they are fully up-to-speed with case law, developments, and regulations relating to ESI. Less than half (43%) believe they have a fairly good understanding but could benefit from more knowledge, and 31% of respondents feel they have little understanding or have never heard of it.

With the changes to the Federal Rules of Civil Procedure in the United States regarding electronic discovery, in-house counsel who are not fully aware of the requirements and complexities risk putting their organizations in jeopardy if they do not rely heavily on outside law firms or experts. U.S. legal teams are concerned about the reality of the ESI explosion, with more than one-fifth (21%) stating that managing colossal volumes of data will be their biggest challenge over the next five years.

Computer-Assisted Forensic Techniques

Within the last ten years, the world of electronic or digital evidence has evolved to become a vital part of practically every case a forensic accountant handles. Most cases require an inquiry into all forms of communications and records of every nature, especially those that are in digital form or were created electronically.

Businesses typically generate hundreds or thousands of documents related to various areas of operations, for instance, thousands of sales invoices, thousands of purchase orders, and thousands of checks. Thus there could be thousands of documents related to an area being investigated for fraud.

The computer can be used to perform investigative procedures on accounts payable and payroll fraud, such as printing out all unauthorized check numbers or checks over a specified amount, printing out a list of all employees not electing insurance or other employee benefits (this might signal a fictitious employee scheme), or identifying vendors that always submit the latest bid or obtain a disproportionate share of contracts.

For example, an investigator investigating for accounts payable fraud might examine payments to vendors for certain attributes, such as by checking vendor names on checks written to an approved vendor list and searching for checks with different addresses for the same vendor names.

Other examples of investigative procedures that can be performed using computers include the following:

- Recomputing items on documents for mathematical accuracy
- Searching for fictitious names or addresses by comparing data on documents to known fictitious names or addresses, for multiple names to the same address, or for multiple addresses for the same name
- Searching for payments made or inventory shipped to a vendor or customer with the same address as an employee
- Searching vendor payments for duplicate payments (The suspect intercepts and retains the duplicate payment.)
- Searching for unusual patterns on purchase orders or contracts, such as unusually large numbers or amounts.
- Searching for unusual accounting entries, for example, debit entries to accounts that normally receive credit entries (such as accounts payable or long-term debt) or credit entries to accounts that normally receive debit entries (such as loans receivable or inventory).

The company's general ledger software package usually will include transaction reports that can be used to identify all transactions affecting an account during a specified period. These reports can be scanned to help identify unusual items. Also much of the publicly available information exists in databases that can be accessed by computer. This can make the data gathering process more efficient.

Third-Party Ethics and Compliance

With the growth of outsourcing and offshoring, many companies are addressing the need to ensure that the third-parties they deal with have effective compliance and ethics programs.

Many companies have begun to examine whether they should initiate efforts or make greater efforts to extend compliance and ethics standards to third parties with whom they have an ongoing relationship. Such third parties include suppliers, distributors, agents, and joint-venture partners. How far should corporate compliance and ethics programs go into an organization's chain of relationships? The need for partners in global markets and the competitive and external pressures from governments, international organizations, and nongovernmental organizations are resulting in increasing company focus on third-party business conduct. As outsourcing and offshoring continue to grow, the issue becomes increasingly important. The issue is further complicated by the need to comply with the Sarbanes-Oxley Act of 2002, as well as by the reports of recent incidents related to product quality and recalls.

In response to these pressures, "many companies have increased their internal focus on programs related to compliance and ethics," says *Supply Chain Digest*. Even some large companies are challenged by the need to drive their standards down to suppliers, according to a recent study by consulting company Integrity Interactive.

Companies are already challenged by financial and operating issues in dealing with a long supply chain. Problems and questions, however, can be exacerbated when it comes to ethical issues. The Integrity survey found, for example, that 78% of companies do not include suppliers in their company compliance and ethics programs, and nearly 58% were not sure if their company regularly assessed ethics risks in the supply chain. The survey also found that 56% of respondent companies do not audit supplier compliance with the standards set in codes they must comply with, which could relate to such things as labor conditions and pay.

Third Party Ethics Management?

To help align suppliers' business conduct with buyers' standards, an organized approach through strategies, programs, and metrics has been developed, which some call "supplier ethics management." The goal is to have "suppliers operate consistently with a customer's corporate policies around ethics, operating conditions, sustainability, and other elements."

However, "the practicality of such a concept can be elusive," says *Supply Chain Digest*, because "companies have widely varying ethical standards, codes of conduct, and other compliance-related program elements." Furthermore, in a global economy, requirements can be various and even contradictory. And in countries with growing economies, manufacturers may "feel less pressure to kowtow to various ethics mandates issued from companies located there."

Employee Codes of Practice

The most common method for handling third party ethics and compliance issues is to adopt and stick to a code of practice or policies that governs the manner in which a company's own employees deal with third parties, according to a report released Feb. 12, 2008 by The Conference Board.

The Conference Board and the Ethics and Compliance Officer Association surveyed 169 companies on the essentials of corporate third party ethics programs. Ninety-five percent of the companies said that although it is vitally important to address third party ethics and compliance issues through codes of conduct for their own employees, they are less inclined to involve third parties directly in these programs.

"With the exception of help lines or whistleblowing systems, the direct inclusion of third parties in companies' ethics and compliance programs is the exception, not the rule," said Ronald E. Berenbeim, principal researcher at The Conference Board and author of the report with Rebecca Walker, an attorney specializing in corporate compliance and business ethics. "Nevertheless, companies are growing more dependent on third party relationships for the achievement of business objectives—either via joint venture, which may be mandated for entering into a new country, or working with suppliers or contractors."

One Size Fits All?

In addition, written policies applicable to specific third parties are not common. In more than two-thirds of the responding companies (69%), the standards for third parties apply in the same manner to all third parties. Among the companies that had policies for specific third parties, contractors and agents are most likely to be mentioned.

"Companies struggle with the competing tensions that arise from developing business relationships with local partners that aren't always mindful of or responsive to a broad range of stakeholder concerns, such as environmental compliance, health and safety, and human rights," according to Walker. "Global organization and nongovernmental organization pressures with respect to these issues also increase the need for companies to address third party ethics and compliance."

Third-Party Compliance and Ethics Practices

Companies prefer doing background or due diligence checks to insisting that the third party adopt the company's ethics and compliance programs or maintain its own system. Seventy-seven percent of respondents perform checks on certain third parties before entering into a business relationship; 74% scrutinize agents; and about half subject all categories of third parties to due diligence. Due diligence searches are more likely to focus on disabling financial or legal conditions than reputation impairments.

The most common component of ethics programs that companies extend to third parties is offering employees of third parties an opportunity to report ethics or compliance related concerns. Almost all programs (98%) rely on the same means used for a company's own employees to report suspected misconduct, rather than a separate system for third parties. The most popular mechanisms are e-mail addresses (65%) and help lines.

Risk Assessment

Approximately 60% of survey participants address third party risks in their company's risk assessment. Agents, suppliers of services, and

contractors are the most frequent subjects of these evaluations; suppliers of goods are somewhat less often subject to scrutiny. Companies are evenly divided as to whether the risk assessment is part of a broader enterprise risk process or limited to ethics and compliance risks.

Training

Ethics and compliance training programs are the third most frequent step that survey participants take in extending their own program to third parties. Slightly more than one-third (38%) of survey participants offer, but don't insist on, some kind of training program for third parties. Most of these programs devote some discussion to the company's own code. In almost every case, those parties that are asked to adopt or certify to the company's internal code of conduct are offered some form of training.

Company audits of third party compliance with ethics policies and practices are infrequent, and a majority of the companies that audit don't do so routinely. Slightly more than 35% of the survey participants perform audits or otherwise verify that third parties conduct themselves as required by the company's own compliance and ethics policies. Of this group, slightly less than half conduct audits on a routine basis, while the remainder focus their audits on specific concerns.

The surveyed companies showed little interest in the third party's own ethics programs. Slightly more than one quarter of the survey respondents ask third parties whether or not they have them, but only 14% of respondents ask for documentation. Companies are especially likely to seek information on the third party's compliance program when considering an acquisition or a joint venture.

Room for Improvement

"The survey suggests that companies are satisfied with current methods of seeking to extend ethics and compliance standards or requirements to third parties but are willing to search for new approaches," says Berenbeim. "Companies rated all ethics and compliance efforts within a narrow and not especially positive range—they deemed them somewhat effective."

The implementation of a means for third parties to report concerns or misconduct was ranked as the easiest means of ensuring appropriate third party compliance; monitoring third party behavior for compliance (arguably one of the key objectives for establishing such a system) was rated by far the most difficult.

For Further Reading:

Finding the Right Balance: The Essentials of Third Party Ethics Programs
Research Report #1416-08-RR, The Conference Board

The report is free to Conference Board members. To download or purchase the report, go online to **http://www.conference-board.org/publications/describe.cfm?id=1427**.

"Supply Chain Trends: How Far Should Corporate Compliance and Ethics Programs Go into the Supply Chain?" *Supply Chain Digest* (February 6, 2008)

The article is posted online at **http://www.scdigest.com/assets/On_Target/08-02-06-3.php?cid=1473?cid=1473&mode=print.**

Simple Solutions to Deter Fraud

CPAs know that various internal controls can help to deter fraud in organizations. However, the recent scandal concerning the French bank Société Générale illustrates the obvious corollary: To be effective the controls need not only to be in place, but also to be implemented.

"The simplest solutions usually work best," comments *The Wall Street Journal* ("Too Many Days on the Job," January 29, 2008), pointing out that the fraud in the Société Générale case may have been avoided had password protection been better and safeguards against fabricated hedges and counterparty risk controls in place. "But," says the *Journal*, "the best way to catch a bank fraudster might just be something more mundane: a forced vacation."

Société Générale claims that it tried several times to make the fraud perpetrator take time off, but gave in to his excuses not to do so. A rule of thumb applied by many large Western banks is that traders be required to take off for at least five consecutive workdays. Some banks require ten days. The reason is detecting fraud is more likely when someone else is handling the order book.

Trickling Down

The alleged fraudster was relatively low in the Société Générale organization. Although the focus in recent years has been on the criminal acts of top executives, in an article in *CFO.com* (January 31, 2008), David M. Katz says that "today's fraudsters are more likely to come from middle management than the C-suite." He attributes this change to implementation of Section 404 of the Sarbanes-Oxley Act of 2002.

What can CPAs do to discourage rank and file management from perpetrating fraud and to detect fraud? Katz offers the guidance of Yigal Rechtman, head of the forensic accounting department for audit firm Buchbinder, Tunick, and Company in "How to Nab the Rogues: 10 Fraud Tips." At the top of the list of tips are "Avoid relying on budgets, install an anonymous tip line, and get credit reports on employees."

To read the discussion of these tips and the other seven tips, go online to **http://www.cfo.com/article.cfm/10600143?f=home_featured**.

AICPA Guidance

In addition, the AICPA offers an array of resources and tools to help CPAs and other professionals combat fraud whatever their role in business. To access this guidance, go online to the AICPA Antifraud and Corporate Responsibility Center at **http://antifraud.aicpa.org**.

At this website, note that in the left-hand box is a link to information about the *AICPA Handbook of Fraud and Commercial Crime Prevention*. This comprehensive handbook provides details, tools, and guidance on many areas of fraud prevention and detection.

Helping Experts Keep Up to Date

A synopsis of the 2007 AICPA National Business Valuation Conference

Without question, the 2007 AICPA National Business Valuation Conference brought attendees up to speed on the technical knowledge and issues relevant to valuation, most of which are critical to valuation analysts' maintaining their skills. Held in New Orleans from December 2–4, the conference offered 34 sessions plus 5 "early riser" sessions organized into 5 tracks: emerging/hot, fair value, litigation, fundamentals, and niche. In addition, 4 preconference optional workshops took place before the main conference.

Robin E. Taylor, chair of the conference steering committee, welcomed the more than 1,000 CPAs who attended. After the welcome, Taylor, now chair of the AICPA Business Valuation Committee, introduced the keynote speaker, Loren C. Scott, Ph.D., president of Loren C. Scott & Associates, Baton Rouge, LA. In his speech, "The Economics of Disasters: The Economic Impact of Katrina and Rita," Scott described the economic impact of the hurricanes in Louisiana and explained why some regions and industries rebounded more quickly than others. Very dynamic and detailed in his presentation, Scott offered insight into how and why the affected areas varied in their ability to rebound. Much of what he told attendees is posted on his firm's website (**http://www.lorenscottassociates.com**) in a report titled, "Advancing in the Aftermath: Tracking the Recovery."

Given the technical nature of most of the conference sessions, a brief summary of any of them could not convey the value of their information and guidance. As Yogi Berra might have said, "You had to be there to be there." However, this article offers an overview of the session topics along with a few tips that presenters offered. Despite the lack of detail, this article also hopes to convey the breadth of guidance offered by experts involved in valuation.

Evergreen Education

Some conference sessions are perennials, focusing on bringing practitioners up to date, such as was done by Mel H. Abraham of Simi Vally, CA in "Here Comes the Judge! Valuation & Case Law Update." Another example is the "Healthcare Valuation Developments, Challenges, and Solutions in 2007—Panel Discussion" moderated by Cindy Eddins Collier, Valuation Solutions, Myrtle Beach, SC with panelists Mark O. Dietrich of Framingham, MA and Don Barbo, HSSK Group, LLC, Dallas, TX.

Fair Value

Among the emerging/hot topics, *fair value* often took center stage. Fair value was covered in several main conference sessions beginning with a "Fair Value GAAP GAAS Overview" presented by Mark Zyla, Acuitas Inc., Atlanta, GA. Zyla covered a great deal of territory in his presentation, providing an overview of fair value accounting, its history, and the need for it in valuations for financial reporting, along with an overview of the relevant rule-making bodies. Early the next day, fair value was the focus of a panel discussion moderated by James R. Hitchner, The Financial Valuation Group, Atlanta, GA with panelists Yassir Karam, Clifton Gunderson LLP, Indianapolis, IN, and Mike Mard, the Financial Valuation Group, Tampa, FL. Mard is one of eleven appraisers in the FASB's Valuation Resource Group. In addition, Mard, along with Hitchner and Stephen D. Hyden, is a co-author of *Valuation for Financial Reporting*, 2nd edition (Wiley). Later in the day, Mard presented "Hot Topics in Fair Value." Also Neil J. Beaton and Robert E. Duffy, both with Grant Thornton, touched on fair value in their presentation on "IRC 409A and SFAS 123R Valuations."

Mard and Karam also covered the subject of fair value in "Valuation for Financial Reporting Case Study Workshop," a three-hour preconference optional workshop, which was scheduled the morning before the main conference opened.

Rereading Revenue Ruling 59-60

As he opened his session, "Dream the Impossible Dream: Can Specific-Company Risk Really Be Quantified?" Gary Trugman, as he often does, advised attendees to read Revenue Ruling 59-60 "once a month." "Every time I read it, I find something new," he added. (The text of RR 59-60 is available on the Trugman Valuation Associates, Inc. website at **http://www.trugmanvaluation.com/RevRul5960.html**.)

Trugman's advice led into the topic of his presentation, determining a company-specific risk premium in developing appropriate discount rates. He cited "a new kid on the block that's worth looking at," the Butler Pinkerton Model™ Company-Specific Risk and TCOE Calculator™ and called it "an addition to the profession."

Presenting Convincing Conclusions

The sessions covered mostly technical information needed by valuation analysts, focusing on specific technical topics and issues. But the lessons learned also covered practical issues that valuation analysts face in presenting the results of their analyses. They included, for example, "ten commandments" for the first-time expert witness, guidance on presenting expert testimony visually, and dos and don'ts for tax valuation trials.

The need for guidance for valuation analysts in presenting their conclusions convincingly was pointed out by Nancy Fannon of the Fannon Valuation Group, Portland, ME and Jim Alerding, Clifton Gunderson, LLP, Indianapolis, IN. The title of their presentation, "Expert Witness Advocacy—Guilty Until Proven Innocent," describes what expert witnesses often face when presenting testimony: a belief of some judges and juries that experts lack objectivity in developing their conclusions.

Fannon and Alerding described "the environment we work in" as follows: "We work within a process that seems predisposed to naturally assume that people are not telling the truth and actively seeks a justification for a centrist view."

They add that this is "perhaps the result of years of listening to he said-she said, hiding the ball, spinning the truth, and wildly divergent views of reality."

Fannon and Alerding also pointed out that the new AICPA Statement on Standards for Valuation Services (SSVS No. 1) addresses the issue of independence in performing valuations (see paragraphs 14 and 15) as does the AICPA Statement on Standards for Consulting Services.

Avoiding Challenges

Guidance on avoiding challenges to expert testimony and being convincing in presenting conclusions, particularly valuation conclusions, came from presenters who make judgments about the quality of the testimony or reports presented by valuation analysts. Brenda Woolbert, the Internal Revenue Service (IRS) team manager for engineers and appraisers, projected on the screen a list of items of questionable appraiser conduct that could provoke an IRS challenge to the appraiser's conclusions. It's hard to believe that most experienced valuation analysts would be guilty of making these errors. However, the errors listed can provide insight for analysts who need to evaluate others' valuations. These items include the following:

- Assuming facts that do not exist
- Purposefully excluding a valuation approach that produces credible results
- Ignoring strong market evidence
- Presenting false information
- Including assumptions as to future events that are implausible
- Assuming forms of ownership that do not exist
- Intentionally disregarding professional standards of appraisal practice
- Participating in an appraisal that results in a value determination intended to reduce tax without objective and credible evidence to support the appraisal

Woolbert said that the IRS was developing a website for valuation analysts, which would provide such future guidance as that related to 6695A penalties. Woolbert also said she expected that the AICPA's SSVS No. 1 would meet with the compliance criteria of Notice 2006-96.

Judge Laro's Lessons

The main conference ended with the presentation, "A View from the Bench: The Biggest Mistakes Experts Make and a Judge's View on How to Avoid Them." The speaker, Judge David Laro, has served on the U.S. Tax Court since 1992. After describing the structure of the tax court, the judge offered valuation analysts some tips in response to moderator Ronald L. Seigneur of Seigneur Gustafson LLP, Lakewood, CO, who asked the judge to identify the top mistakes were that experts made in their testimony. The mistakes Judge Laro mentioned included the following:

- Conflicts of interest.
- Lack of independence. Related to the mistake of having a conflict of interest is allowing yourself to be influenced by the people who hire you.
- Lack of confidence. Laro cited a case in which the appraiser was criticized because he came from Alaska to do an appraisal and stayed only two days. Laro said, "It doesn't matter how long, but how you did your job."
- Weak analysis. The mistakes may be in the report itself. Laro noted that reports are becoming more complex. He also noted that they may be weak on analysis, although strong on data. The valuation analyst needs to show how the data tie into the conclusion.

Judge Laro offered further guidance on appraisers' reports. He said that the report is tantamount to direct testimony by the appraiser and that whatever is not in the report is not evidence. Something left out is an omission.

An appraiser also needs to present his or her credentials in the report. Furthermore, the report needs to state upfront that the valuation is a fair market value valuation. And again the valuation analyst needs to show how the data and analysis lead to the valuation conclusion.

Bigger and Better

This year's conference will be sponsored jointly by the AICPA and the American Society of Appraisers (ASA). The AICPA/ASA Joint Business Valuation Conference is scheduled for November 10–12, 2008 at the Bellagio Hotel, Las Vegas, NV. Note that Monday, November 11 is Veterans Day in the United States and Remembrance Day in Canada. For more information about this event, call 888-777-7077 or access it online at **http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/BusinessValuationandLitigationServices/Engagements/PRDOVR~PC-BVAL08/PC-BVAL08.jsp.**

FYI...

Does Fraud Speak for Itself?

Preliminary findings from research conducted by Patrick Fan and Greg Jenkins, associate professors of accounting and information systems in the Pamplin College of Business, suggest that a technique used extensively in the social sciences to scrutinize written and oral communication may be used for detecting fraud. The technique can be used to identify language patterns in management communications that are inconsistent with either the company's financial performance or with the communications of other companies in the same industry. Such inconsistencies may indicate fraud.

"The results of our initial analysis suggest that our model has substantial predictive power," says Jenkins. "When fraud is committed in companies, there appear to be patterns in corporate communications that imply wrongdoing."

Fan and Jenkins hope to develop their methodology, based on knowledge from auditing and information systems, into a more precise new tool to help auditors and regulators detect fraud. PricewaterhouseCoopers has given them a grant of about $196,000 for their project, which is expected to be completed in 2009.

Jenkins, a former auditor at Ernst & Young, currently serves on a research task force that is providing guidance to the Public Company

Continued on page 8

Continued from page 7

Accounting Oversight Board on matters related to audit firms' quality control. Firms, Jenkins says, are working to develop more sophisticated fraud detection techniques. He and Fan hope to reduce the financial resources and the human effort required in auditing with a computerized tool to handle the tedious, time-consuming, and often impossible task of manually examining all available text documents from the firm being audited.

Their model uses text mining techniques to identify word patterns associated with financial fraud. By recognizing language patterns or trends that are inconsistent with either the company's financial performance or communications issued by other companies in the same industry, the software would guide auditors to particular areas—revenue recognition policies, practices, or disclosures of liabilities, for example—that may need further examination.

Benchmarking a company's communication patterns against those of other companies in the same industry may help reveal unusual or unexpected differences. Jenkins says that a company's financial performance may be similar to that of its competitors, "yet the language it is using to describe its prospects seems overly optimistic or overly specific or vague relative to others in the industry." For example, from the late 1990s, Enron exuded an "unlimited optimism" while other companies were starting to struggle. Jenkins says that Enron's descriptions of its prospects were inconsistent with those of its competitors. Furthermore, Enron's "descriptions of related-party transactions were incomplete and overly vague."

"We're tracking tens of thousands of words from multiple companies and multiple periods," Jenkins says. "We're using computing power to go through and look at language to identify patterns—words and frequency of usage—that would be very difficult for a human reader to discern. Our findings so far show that there are systematic differences in textual communications between the two groups of companies."

He and Fan envisage their software as serving as a decision-support tool that would improve the efficiency of the auditing process, help auditors gain additional sources of evidence, and, ultimately, enable detection of financial fraud.

AAA Forensic Section Proposed

Larry Crumbley, editor of the *Journal of Forensic Accounting*, is attempting to start a Forensic and Investigative Accounting Section as part of the American Accounting Association. According to Crumbley, the proposed section will "identify issues in forensic auditing, fraud investigation and deterrence, evidentiary basis, valuations, computer forensics, and litigation support."

"The reason this is important to accountants," says Jim DiGabriele of DiGabriele McNulty, West Orange, NJ, "is that this will surely—and finally—be an area where academics and practitioners can further the discipline through collaborative research."

Crumbley can be contacted at 225-578-6231; 225-763-6409; fax: 225-578-6201; email: dcrumbl@lsu.edu.

AICPA FVS Section

American Institute of Certified Public Accountants
Forensic & Valuation Services Section
220 Leigh Farm Road
Durham, North Carolina 27707-8110

ADDRESS SERVICE REQUESTED

ISO Certified

First-Class Mail
U.S. Postage Paid
Riverdale, MD
Permit No. 5165