The Forensic Examiner is the official peer-reviewed journal of the American College of Forensic Examiners International that contains periodic forensic accounting articles.
www.theforensicexaminer.com

Fraud Magazine is a bi-monthly publication by the Association of Certified Fraud Examiners that gives readers practical "down-in-the-trenches" information.
www.fraud-magazine.com

Journal of Forensic Accounting (2000-2008) was an independent international forum for the publication of research dealing with the models and methodologies of investigative and forensic accounting, seeking to establish a balance between theoretical and empirical studies, and striving to foster practitioner-academic dialogue and collaboration.
www.rtedwards.com/journals/JFA/students.html

Journal of Forensic and Investigative Accounting is a bi-yearly electronic magazine started in 2009 that publishes original creative and innovative academic studies with some practical articles. Published by Larry Crumbley at Louisiana State University.
http://www.bus.lsu.edu/accounting/faculty/lcrumbley/jfia/Default.htm

Journal of Forensic Studies in Accounting and Business provides an outlet for communication and research collaboration among fraud and forensic accounting practitioners and education programs. Published by Georgia Southern University.
www.fraudforensicacct.org

The Forensic and Valuation Services Center (AICPA) provides members with up-to-date sources of professional guidance and tools available.
http://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/Pages/default.aspx

The Value Examiner is an independent, professional development journal published bi-monthly by the National Association of Certified Valuation Analysts, containing substantive, peer-reviewed articles in business valuation, forensic accounting, fraud risk management, and other topics.
http://www.nacva.com/examiner/examiner.asp

¶ 1135 AMERICAN ACCOUNTING ASSOCIATION FORENSIC ACCOUNTING SECTION

After a struggle over a number of years, Larry Crumbley was able to obtain 500 signatures, and the American Accounting Association agreed to allow a new section called Forensic and Investigative Accounting (FIA). The FIA section is dedicated to the continual improvement of forensic accounting research and education, through the encouragement, development, and sharing of:

- The promotion and dissemination of forensic and investigative academic and practitioner research.
- The relevant and innovative curricula with an emphasis on effective and efficient instruction.
- The exploration of knowledge-organization issues related to forensic accounting programs.
- The creation and presentation of CPE courses to members and professionals.

Forensic and investigative accounting often intersects with other professions including those of the law, criminology, sociology, psychology, intelligence, information technology (open sourcing, cyber-crime, digital evidence, data mining, and IT systems and control), computer forensics, and other forensic sciences. Graduate students may wish to be associate members, and practitioners could become full-time members.

¶ 1141 FOREIGN CORRUPT PRACTICES ACT

Following investigations by the SEC as a result of the Watergate scandal, over 400 businesses were found to have paid over $300 million in bribes coming from slush funds to foreign governmental officials and politicians. As a result of these discoveries by the SEC, the Foreign Corrupt Practices Act (FCPA) was enacted as a federal law in 1977. The FCPA prohibits companies from paying corrupt bribes to foreign government officials and political figures for the purpose of obtaining or retaining business.

The purpose of the FCPA is to combat corrupt business practices such as bribes and kickbacks. Thus, for more than 35 years these foreign bribery laws in the United States have restricted all U.S. employees, regardless of where the business is conducted.

FCPA prohibits corrupt payments to foreign officials for the purpose of obtaining or keeping business, or directing business to anyone. These laws apply to foreign firms and persons who take any act in furtherance of such a corrupt payment while in the United States. Companies whose securities are listed in the United States must meet FCPA. Also, FCPA prohibits corrupt payments through intermediaries.

There are two provisions to the Foreign Corrupt Practices Act. First, the anti-bribery provision, which is enforced by the Department of Justice and second, the accounting provisions, which are enforced by the Securities and Exchange Commission (SEC). The FCPA prohibits any U.S. citizen, U.S. business, foreign corporations trading securities in the U.S., or foreign persons or entities currently in the U.S. to make corrupt payments to foreign governmental officials directly or through an agent in an effort to obtain or retain business.

A government official can be any government employee and may even extend to employees of state owned businesses. A payment can consist of anything of value, but such payment must have corrupt intent to improperly influence the governmental official.

Under the books and records provision, issuers of U.S. securities are required to make and keep books, records, and accounts that accurately reflect the issuer's transactions and disposition of assets. Under the internal controls provision, issuers must devise and maintain a system of internal controls sufficient to assure managements control and responsibility of the firm's assets. These two provisions do not only apply to bribe-related violations.

Often bribes are concealed under accounts such as consulting fees or traveling expenses. In instances in which all the elements of the anti-bribery provision cannot be proven, often the companies are still liable under the accounting provisions.

The FCPA covers both issuers and domestic concerns. Issuers includes any U.S. or foreign corporation that has a class of securities registered in the U.S, or that is required to file reports under the Securities and Exchange Act of 1934.

Domestic concerns refers to any individual who is a citizen, national, or resident of the United States and any corporation and other business entity organized under the laws of the United States or of any individual U.S. State, or having its principal place of business in the United States.

During 2010 alone, the Securities and Exchange Commission and Justice Department reached settlements with 23 companies for alleged violations of the law, collecting a total of $1.8 billion in financial penalties. For more detail, see A Resource Guide to the U.S. Foreign Corrupt Practices Act, by the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission. Listen to http://www.justice.gov/criminal/fraud/fcpa/guide.pdf

[101] Oracle Corporation was charged by the SEC with violating the FCPA by failing to prevent their Indian subsidiary firm from secretly setting aside money off their books that was then used to make unauthorized payments to phony Indian vendors.

An Oracle Corporation subsidiary, Oracle India, sold software licenses and services to the government of India through local distributors. Over a dozen times between the years of 2005 and 2007, Oracle India structured payments with the Indian government in a way that allowed Oracle India's distributors to keep approximately $2.2 million in unauthorized funds off Oracle India's books. The distributors were told to keep excess funds for "marketing development purposes." The distributors were then instructed to make payments ranging from $110,000 to $396,000 to various third party vendors that provided no actual service to Oracle India and were

Overvalued Assets or Undervalued Expenses and Liabilities

What Is This Method?

Overvalued assets comprise property for which fraudsters set prices that are unsupportable using standard business valuation approaches. These assets might be bought to essentially pay off parties to which the fraudsters are beholden, sold to artificially boost income, or simply held and recorded on statements at far more than their actual worth.

Gain-on-sale accounting is a technique enabling fraudulent executives to use SPEs to purchase or sell overvalued ventures at unsupportable values, which are recorded by the corporation as massive losses/revenues.

Accounts receivable offers myriad opportunities for valuation schemes. GAAP requires accounts receivable to be reported at net realizable value—the gross value of the receivable minus an estimated allowance for uncollectible accounts. Companies circumvent GAAP rules by *underestimating* the uncollectible portion of a receivable. Underestimating the value of the provision (the amount deemed uncollectible) artificially *inflates* the receivable's value and records it at an amount greater than net realizable value. A related fraud is failing or delaying to write off receivables that have become uncollectible.

How Do Perpetrators Use This Scheme?

In 1998, General Electronic Company underaccrued warranty obligations by $100 million for a series of gas-fired turbines used in power plants. The turbines had a design flaw.

Pension funds lend themselves to undervaluing of liabilities. In the 2002–2003 stock market decline, many companies understated their pension expenses.

Finally, Enron committed this type of reporting fraud as well. Its Braveheart SPE was designed to book a gain-on-sale income on an abortive deal between Enron and Blockbuster Inc. The video giant was to develop and market an on-demand movie product through an Enron-supplied broadband fiber system. Six months after the project was signed, the system still had no paying customers and was only in the testing phase. Although traditional accounting rules would allow no profits to be shown, Enron "sold" the joint venture to Braveheart thereby recognizing $111 million net gain, reported in Q4 2000 and Q1 2001. The venture never came to fruition, dying a swift death in its test markets.

Although GAAP requires expenses to be recognized in the period in which they are incurred, Symbol Technologies, Inc. deferred $3.5 million of FICA expenses to a later year in order to boost its net income.

Omitted Liabilities

What Is This Method?

Omitted liabilities are the mirror image of fictitious revenues and assets: fraudsters hide debt or employ other off-balance sheet financing to avoid having to include the negative picture on corporate financial statements. SPEs may be used to bury poorly performing assets because their transactions are not part of the corporate financial statements.

How Do Perpetrators Use This Scheme?

By the time Enron declared bankruptcy in December 2001, it was reported to have hidden billions of dollars of off-balance sheet debt using SPEs. Also, Enron entered into futures contracts with financing organizations such as J.P. Morgan that were thinly disguised loans not actually based on delivery of energy commodities.

Enron also used *prepaid swaps* through its Delta subsidiary wherein CitiGroup paid the fair value of its portion of the swaps but Enron was allowed repayments spread over five years—in effect, obtaining loans. Enron never disclosed these transactions as such on its financial statements, accounting for the deals as "assets from price risk management" and as "accounts receivable."

Omitted or Improper Disclosures

What Is This Method?

Disclosure, one of the categories of management assertions in financial statements, requires that certain information, such as assets held as collateral and preferred stock dividends in arrears, be included in the notes to financial statements. Fraudsters use *omitted or improper disclosures* to avoid listing questionable or bad news on the balance sheet. For example, contingent liabilities may be underestimated and their likelihood of loss may be understated to minimize their financial statement effect.

Improper disclosures can take the form of misrepresentations, intentional inaccuracies, or deliberate omissions in: descriptions of the corporate or its products, in media reports and interviews, as well as in financial statements/annual reports. Omissions may also occur in management discussions and other nonfinancial statement sections of annual reports, 10-Ks, 10-Qs, and other reports; as well as in footnotes to the financial statements.

How Do Perpetrators Use This Scheme?

Enron used subsidiaries and SPEs as a "parking lot" for assets and losses the corporation's managers wished not to reveal on Enron's financial statements. Andrew Fastow, Enron's CFO, managed the LJM1 and LJM2 SPEs to hide charges in Enron's accounting treatment of gas supply contracts and to inflate accounting income. Enron thus began transacting derivatives deals with companies that were inside Enron. The derivatives were even based on the value of Enron's own stock.

Equity Fraud

What Is This Method?

Equity fraud, also known as *investment* or *securities fraud,* basically involves the promotion and sale of nonexistent or illegal securities investments as well as intentional misrepresentation or concealment of investment and financial related information. Equity fraud causes third parties to suffer financial loss. Equity fraud is usually perpetrated to deceive or mislead and is illegal. The many forms of investment fraud range from boiler rooms, shady stock promotions, real estate transactions, and corporate financial fraud, all of which dupe investors in public companies.

How Do Perpetrators Use This Scheme?

Enron's most publicized equity fraud involved issuing $1.2 billion in stock to a related special-purpose entity and recording a $1.2 billion note receivable for the transaction, rather than a contra account to shareholder equity.

Related-party Transactions

What Is This Method?

According to AccountingBuzz.com, a *related party transaction* is an interaction between two parties, one of whom can exercise control or significant influence over the operating policies of the other. A special relationship may (and often does) exist between the parties, e.g., a corporation and a major shareholder or parent and subsidiary.

How Do Perpetrators Use This Scheme?

Enron became infamous for engaging in many related-party transactions through its special-purpose entities. Through Andrew Fastow's LJM2 SPE, Enron pledged millions of shares of Enron's stock to the four Raptors off-balance-sheet entities. Enron's finance group recorded the Raptors' promissory note as an addition (rather than the correct reduction) to Enron's shareholder equity. The Raptors SPEs absorbed financial results the executives did not wish to reveal on Enron statements, and the corporation wound up taking massive loans to prop up the SPEs' financial status before Enron's eventual bankruptcy.

cluded distributing Purchase Pro software. These warrants gave AOL the right to buy shares in Purchase Pro for a penny, hence booking $20.5 million in advertising and commerce revenue in its December 2000 quarter and another $7 million in the March 2001 period. Thus, AOL recognized a total of $28 million of income.

The Parmalat deceptions illustrate the need to confirm even cash accounts. Parmalat, an Italian dairy company, had a nonexistent Bank of America bank account worth $4.83 billion. A SEC lawsuit asserts that Parmalat "engaged in one of the largest and most brazen corporate financial frauds in history." Apparently, the auditors Grant Thornton relied on a fake Bank of America confirmation prepared by the company.

SAS No. 99 does *not* prohibit clients from preparing confirmations. This fraud continued for more than a decade, and at least $9 billion went unaccounted for. Therefore, the audited company should not be in control of the confirmation process. The owner treated the public company as if it was his own bank account. An unaware phone operator was the fake chief executive of more than 25 affiliated companies. Some $3.6 billion in bonds claimed to be repurchased had not really been bought.

Companies may be tempted to hide debts or liabilities from the balance sheet using these techniques:

1. Using the equity method (rather than trading security and available for sale methods). Nets the assets and liabilities of the investee.
2. Lease accounting (arguing that leases are operating leases). Understates 10 to 15 percent.
3. Pension accounting—netting of the projected benefit obligation and the pension assets. Must un-net them.
4. Hiding debt inside special–purpose entities—trillions of dollars of SPE debt is off the books (e.g., securitization, SPE borrowings, synthetic leases).

Professor Edward Ketz says financial statement readers can make analytical adjustments by searching footnotes for 1, 2, and 3. But there are generally no disclosures for asset securitization, SPE borrowings, and synthetic leases.[100]

Leasing is a favorite way to understate debt on the balance sheet. Airlines have the ability to run their fleet of planes using operating leases whose costs do not have to be fully shown on the balance sheet. David Tweedie, chairman of the International Accounting Standards Board, says his ambition is to fly on an aircraft that is on an airline's balance sheet before he dies.[101]

BAD BALANCE SHEETS. Adelphia acquired a number of companies and as a result increased its debt from $3.5 to $12.6 billion. To improve the balance sheet, the Rigas family created some entities controlled by the family and moved some of the debt onto the special purpose entities without consolidating them. At least $3.1 billion of the debt was owed by the Rigas family, but was not reported on the Adelphia balance sheet.

In a similar fashion, the Baptist Foundation of Arizona (BFA) set up two subsidiaries owned by insiders during the 1989 real estate bubble bust. BFA then sold the depressed real estate to the subsidiaries at book value and recorded notes receivables at the book value amount (and not the FMV). Presto, a cleaner balance sheet.

¶ 4161

PENSION PLAN PROBLEMS

Under pension plan accounting, the expected long-term rate of return (not the actual rate of return or the dollars actually received) is what impacts net income. During rising stock markets, pension fund investments can inflate the bottom line. Small changes in assumptions can make a huge difference in net earnings. Some companies use rates as high as 8 percent, because an upward change of one percentage point can increase the bottom line by more than $100 million.

In 2012, unfunded pension liabilities for private companies were huge, with General Electric having the largest negative liability of $21.6 billion. Companies with more than $10 billion underfunding were AT&T, Boeing, Exxon Mobil, and Ford. At the end of 2011, the value of assets in defined benefit plans in companies in the S&P 500 index was $1.32 trillion, but the value of future obligations was $1.68 trillion, a shortfall of around $355 billion or 22 percent of promised benefits.[102]

The Pension Benefit Guarantee Corporation (PBGC) is a publicly created but privately funded group that insures the U.S. occupational pension plans. In November 2012, the PBGC reported a record gap between available assets and projected liabilities of $34 billion. This shortfall did not consider future premiums or insolvencies.[103]

The inability of the PBGC to set premiums on employers that considers the risk that each company presents keeps the PBGC from stabilizing its finances. The PBGC would like to set premiums on companies like agencies insure deposits at national banks.[104]

Social security is paying out more than the system takes in, and its operating deficit will be more than $800 billion over the next 10 years, and federal and state pension systems also are underwater. The unfunded liabilities for federal employees total more than $630 billion, and state pension plans are underwater by at least $100 billion. All total, unfunded pension liabilities add at least $2.5 trillion to U.S.'s $17 trillion Federal debt and the state and local debt of $2.8 trillion.[105]

¶ 4171

RESERVE ESTIMATES

Companies may play around with reserve estimates that are found on most balance sheets. Reserves are established to cover future adverse developments, such as warranty claims and bad debts. Because companies have huge discretion as to their size, the smaller the reserve, the less costly to the bottom line.

The SEC sued Xerox in 2002 stating that the company increased its earnings by almost $500 million by placing into income so-called cushion reserves. Xerox agreed to pay a $10 million civil penalty to settle the SEC dispute without admitting or denying wrongdoing with respect to approximately 20 reserves. Then in mid-2002, Xerox admitted that its pretax income was inflated by 3.6 percent, or $1.41 billion over the past five years. The SEC said Xerox artificially booked more of lease revenue upfront rather than over the life of the lease.

In August 2002, bankrupt WorldCom disclosed another $3.3 billion of book cooking on top of the $3.85 billion uncovered in June 2002. This new fraudulent accounting involved reversing a "cookie jar" of reserves for bad debts, taxes, and litigation, sometimes called cookie-jar accounting. One week earlier the company's CFO, Scott Sullivan, and controller David Myers were arrested and charged with hiding at least $4 billion of expenses and lying to investors and regulators.[106]

Reserve reversing is common, especially after a merger. A company will overestimate a merger/acquisition reserve, and then inflate earnings after the merger. CUC International (later Cendant) overstated its merger/purchase reserves.

- A company must disclose any clawback policies for any compensation-based incentives that were paid out based on any erroneous financial information reported under the securities rules.
- Companies must seek recoupment from any current or former executive officer of any incentive-based compensation paid during the three-year period preceding the date that the corporation is required to prepare an accounting restatement that was based on any erroneous data.

Research by three professors found that clawback provisions resulted in significant improvements in both actual and perceived financial reporting quality. They also found an increase in CEO compensation after adoption of new clawback provisions.[179]

Deutsche Bank AG clawed back around $53.5 million in bonuses from a former trader who was involved in attempting to rig interest rates while working for the bank. The trader dealt in derivatives and was paid a percentage of the profits that he made with deferred compensation by a mixture of cash and stock.[180]

Validating Early Fraud Prediction Using Narrative Disclosures

While fraud continues to increase over the years, so have the consequences of fraudulent activity. Companies are more at risk than ever with huge fines being levied (often toping $100 million). There is a need for a timely, accurate predictor of fraudulent activity that will allow fraud to be mitigated.

Chih-Chen Lee, Natalie Tatiana Churyk, and B. Douglas Clinton developed an early fraud prediction method that they claim to be more accurate, more useable by a variety of interest parties, and able to be applied earlier than traditional financial, quantitative fraud predication models. C.C. Lee et al. instead uses a qualitative method to analyze narrative disclosures and, more specific to this study, the Management Discussion and Analysis section of the annual report for signs of fraud. They identified ten narrative variables that were significantly different between fraud and non-fraud companies. Out of these ten, four factors were determined to provide the strongest prediction of deception. Using these four factors, logistic regression and a cross validation procedure, the model accurately classified firms with and without fraud 64.8 percent of the time. Using a holdout sample the model accurately classified the firms with and without fraud 55.9 percent of the time. Tradition fraud prediction models have reported success rates of 30-40 percent.[181]

The four factors used by the model are[182]

1. Fewer terms indicating positive emotion.
2. Fewer present tense verbs.
3. The presence of an increased number of words.
4. Fewer colons.

Deceivers often evidence negative emotions that reflect a negative experience and/or an attempt to disassociate themselves from the experience or message. Deceivers also subconsciously avoid using present tense as another way of disassociating themselves from a deceptive message. Deceivers try to avoid using clarifying language and purposely structure sentences to make interpretation difficult and unclear. Consequently, they tend to avoid colons as they often precede clarifying examples. The expectation of an increased word count stems from the fact the deceiver will take extra time to attempt to be directionally persuasive and more convincing in hopes of avoiding being caught.[183]

The three professors believe that their model will help discover fraud earlier, before it has already caused disastrous financial damage.[184] Their research shows that post-SOX content analysis is still valid even though firms may have tried to over-manipulate the easy to adjust variables such as "for example."[185]

¶ 4246

CONCLUSION

In the absence of internal auditors and external auditors who take responsibility for fighting fraud, the forensic accountant must step into this void. The SEC seems to be moving the traditional players in line, but despite improvements in fighting fraud on all sides, there will be a need for forensic accountants who are specially trained and more suited personality-wise to remain independent and detect and fight fraud. These specialists may become part of one of the auditing teams or may be engaged separately. A comparison can be made between a forensic accountant and a management consultant. Whereas the skilled management consultant arrives from the outside and cuts through the personalities to make the tough calls about waste and assess things like customer focus, marketing prowess, proper infrastructure, and sales organization effectiveness, the forensic accountant can be engaged to take an independent look at controls, systems, personnel, data, etc., to detect fraud.

Efforts of Congress, the SEC, the various stock exchanges, accounting associations and authorities, and others will continue to place more pressure on management, audit committees, accountants, and auditors to fight fraud. Still, the stakes are high and the special skills and knowledge to effectively fight fraud are substantial. Counting on internal auditors and independent public accountants engaged for the financial audit to uncover financial statement fraud in all its complexities is unrealistic. Specialists in fraud detection who possess the required mindset, the proper objectivity, and the required skills will be necessary. Whether these fraud fighters are part of the internal audit team, independent audit team, audit committee, or some yet-unknown entity to approach the problem from another angle remains to be seen.

Although the task is daunting, the fraud-fighting toolset will continue to develop. As more fraudulent activities of the past several years are examined in detail, more inside information will become available and will be used to develop more sophisticated fraud detection skills and techniques. Forensic accountants are needed because the odds that the crime or theft is reported is 2.8 to 1 against.[186]

ENDNOTES

1 Mark Gimein, "What Did Joe Know?," FORTUNE (May 12, 2003), p. 120.
2 Ken Brown, "Auditors' Methods Make It Hard to Catch Fraud By Executives," THE WALL STREET JOURNAL (July 8, 2002), pp. C-1 and C-3.
3 Levitt speech before the Economic Club of New York, New York City, October 18, 1999, *http://www.sec.gov/news/speech/speecharchive/1999/spch304.htm.*
4 Extracted from the "Summary of Conclusions," Report of the Special Audit Review Committee of the Board of Directors of HealthSouth Corporation, May 28, 2004.
5 SEC Rule 10b-5.
6 SAS No. 99, Consideration of Fraud in Financial Statement Audit (New York: AICPA 2002); Rules 3200T and 3500T, PCAOB, 2004, 143-144.
7 International Standards for the Professional Practice of Internal Auditing, IIA, 2004.
8 IIA, AICPA, ACFE, MANAGING THE BUSINESS RISK OF FRAUD: A PRACTICAL GUIDE (2008), p. 5, *http://www.acfe.com/documents/managing-business-risk.pdf.*
9 Discussions on the role of the independent auditor and the following discussion about the internal auditor's role are digested from D.L. Crumbley, J.J. O'Shaughnessy, and D.E. Ziegnenfuss, U.S. MASTER AUDITING GUIDE (Chicago: CCH INCORPORATED, 2002).
10 H.W. Wolosky, "Forensic Accounting to the Forefront," PRACTICAL ACCOUNTANT (February 2004), pp. 23-28.
11 *Ibid.*
12 SAS No. 82, Consideration of Fraud in a Financial Statement Audit (New York: AICPA 1997).
13 George Mannes, "Cracking the Books II: Reliving Equity Funding, Part 2," *TheStreet.com*, accessed October 22, 1999.
14 Larry Neumeister, "Prosecutors Charge Madoff's Accountant with Fraud," YAHOO! FINANCE (March 18, 2009), *http://biz.yahoo.com/ap/090318/na_us_madoff.scandal.html?.v=4.*
15 Mike McNamee and Amy Borrus, "Bill, Show Those CPAs You're the Boss," BUSINESS WEEK (April 28, 2003), p. 84.
16 Adrian Angelette, "Auditors Blamed," BATON ROUGE ADVOCATE (October 23, 2003), pp. A-1 and A-8.
17 H.W. Wolosky, "Forensic Accounting to the Forefront," PRACTICAL ACCOUNTANT (Febraury 2004), pp. 23-28.
18 Public Oversight Board, PANEL ON AUDIT EFFECTIVENESS: REPORT AND RECOMMENDATIONS (August 31, 2000), p. 88.
19 *Ibid*, p. 89.

in *E.C. James*[147] overturned the prior *L. Wilcox*[148] decision and held that embezzled funds are taxable to a thief under Code Sec. 61(a) in the year the funds are stolen. Any stolen assets are not deductible by the employer until the year the thefts are discovered.

The embezzler must report the assets embezzled or stolen in gross income for each year of the theft which requires the filing of amended returns.[149] Essentially, income is taxable at the time the fraudster takes control of the funds, regardless of future restitution or signing a payback agreement.[150] The stolen funds are taxable even if the employer fails to provide a Form 1099. Stolen funds are taxable in the year taken even if the victim institutes proceedings to recover the full amount prior to the assessment of the tax by the IRS.[151] In other words, even in a debtor-creditor relationship, the fraudster still has taxable income. Further, the illegally acquired funds are taxable even if the victim is reimbursed by an indemnity bond. Also, a self-employed fraudster would report the amount on Schedule C and may be subject to self-employment taxes on the illegally acquired income. Further, the fraudster may be subject to interest and penalties by the IRS for non-payment of taxes on the illegal income.[152]

Any included income can be reduced each year by the amount that is repaid to the employer in that particular year. If, as in our example, the repayment is made in a year after the theft, the fraudster may report the restitution amount as a miscellaneous itemized deduction, subject to the two-percent adjusted gross income limitation.[153]

A deduction is not available unless the fraudster can show that the embezzled assets were previously recorded as taxable income. This tax information could be helpful to a forensic accountant in case of legal proceedings.

There may be a limited exception. A Second Circuit decision[154] in 1977 held that an employee does not have to include the illegally acquired funds in income if four criteria are met:

1. Taxpayer fully intended to repay the funds.
2. Taxpayer expects with reasonable certainty that he/she will be able to repay.
3. The person believes that the withdrawals will be approved by the corporation.
4. Employee makes a prompt assignment of assets sufficient to secure the amount owed.

The installment note option probably would not fall into this exception.

Under Code Sec. 165(a), the victim is allowed as a deduction any loss sustained during a tax year that is not compensated for by insurance. Further, Code Sec. 165(e) indicates that the loss is deductible in the year of discovery. However, where a reasonable prospect of recovery exists, no loss is available. "Reasonable prospect of recovery" is a question of facts to be determined upon examination of all of the facts and circumstances.[155] If in the year of discovery there exists a claim for reimbursement with a reasonable prospect of recovery, no loss is deductible until the tax year in which it can be ascertained with reasonable certainty that the reimbursement will not be received.[156] Thus, a signed installment note by the fraudster would postpone any deduction. A victim is required to report the income to the IRS in each year the employee embezzles assets and may not offer to ignore the reporting in return for a signed installment note. Code Sec. 6721 imposes a penalty if a corporation fails to file correct information. An employer's best choice is to report the income on Form 3949A, rather than Form W-2 or Form 1099-MISC. Form W-2 is used to report compensation for work performed, and Form 1099-MISC is used to report payments to non-employees (e.g., awards, commissions, prizes). Informational Referral (Form 3949A) is used to report possible violations of the tax laws, such as unreported income, kickbacks, and false and altered documents.

An employer can provide the fraudster's name, address, social security number, and describe the alleged violation. By providing the amount of illegal income and the tax years, such information could help prove the amount of the theft loss.

Under the facts in our example, if a company does not allow the fraudster to sign an installment note, the company can take a theft loss deduction in the year of discovery reduced by any insurance recovery. The company does not have to show a conviction for theft, but must prove the amount of the theft. Filing a police report could help substantiate the loss. In the case of stolen assets, the theft loss amount is the adjusted basis of the stolen property.[157]

The signing of the installment note stops the victim from taking a theft loss deduction. Each of the $300 payments in the example to the employer is not taxable, but the interest would be taxable. The fraudster could take a miscellaneous itemized deduction.

In our example, the monthly payment is not sufficient enough to even pay the amount of interest due and thus not enough to reduce the loan principal.[158] Thus, the employee will never be able to pay off the loan. Even if the note is doubled to $600 per month, after 12 months the outstanding loan would still be approximately $107,400.

Based upon the above calculations and the unlikelihood of full repayment by a fraudster, the Form 1099 technique may not be a valuable approach. An employer must use an analysis of a current deduction versus a present value of risky future payments to determine whether to go the Form 1099 route. Any installment note should include a reasonable interest rate or the imputed interest rule would apply.[159] The IRS would impute interest income to the victim.

¶5131 CARBON DATING PAPER AND SIGNATURES

Radioactive carbon dating and microscopy analysis may be used to prove the age of a document or the age of a signature. Dating the writing on a document or a signature can corroborate a suspected forgery. Or a stereoscopic microscope may be used to study signatures for forgery.

For example, if a document is dated 9 years ago and the signature or endorsement on the document is more recent, the document is a forgery.[160] The controversy over President Obama's birth certificate could have easily been settled by carbon dating the paper and the ink (as was suggested in a *Philadelphia Inquirer* editorial, April 28, 2001), and investigating the signature. However, no carbon dating and microscopy analysis was apparently done.

EYEWITNESS

In the mid-eighties a West German newsmagazine paid approximately 9 million German marks for 60 small books that were allegedly diaries of Adolf Hitler. Handwriting analysis appeared to demonstrate that the diaries were Hitler's.

The problem was the police used exemplars written by a notorious forger Konrad Kajan. An ultraviolent-light examination showed that the paper contained an ingredient that was not used in paper until 1954. Hitler died in 1945. Forensic tests on the ink revealed that the ink had been applied to the paper within the past 12 months. Forensic accountants can have suspected documents tested.

¶5136 SOCIAL ENGINEERING

Employees must be taught not to be fooled by fraudsters using social engineering schemes that find ways around internal controls. Hadnagy describes social engineering as "the art or better yet, science, of skillfully maneuvering human beings to take action in some aspect of their lives."[161]

There are a number of social engineering schemes which fraudsters may use to get around internal controls. We are all familiar with the phishing e-mails which we receive weekly trying to pry valuable personal information about ourselves. These phishing e-mails often work.

Similarly, pretexting involves an individual lying to obtain privileged information or data. An individual will gain your trust and then attempt to get you social security number, mother's maiden name, and other facts. An example would be assuming the identity of an authority figure by finding a picture and putting it on an identity badge. The Gramm-Leach-Bliley Act of 1999 made certain types of pretexting illegal. Phreaking involves using a similar technique but using the phone.

Dumpster diving involves sifting through companies' dumpsters to find sensitive information. For example, Proctor & Gamble went through Unilever's dumpsters and found 80 sensitive documents. The legality of dumpster diving varies from state to state. Two pre-

- Appropriate form (e.g., in writing)
- Entered into freely

A breach of a contract may occur when a party fails to perform or says he or she will not perform. In either situation, the injured party may sue for damages. Damage calculations are covered in Chapters 10 and 12.

The intentional failure to perform a contract does not necessarily result in fraud. The injured party must show that the other party did not intend to perform the contract and deliberately mislead the other party. For both civil and criminal actions, there must be proof that the party knowingly and willfully knew that the contract was false with the intent to deceive or defraud. With such a heavy burden, it may not be worthwhile to try to prove fraud.

Procurement Fraud Techniques Are Numerous

There are numerous ways to commit procurement fraud, and H.R. Davia outlines these major techniques for engaging in a procurement fraud scheme:[45]

1. Bribes and kickbacks
2. Bid rigging
3. Defective pricing
4. Phantom vendors
5. Product substitution
6. Conflict of interests
7. False claims
8. Cost mischarging
9. Contract specification failures
10. Duplicate, false, or inflated invoices
11. Split purchases
12. Unnecessary purchases
13. Defective delivery

Bribes are universal and are the most damaging of these corrupting schemes. Often bribes and kickbacks are entwined with one or more of the other schemes. Whether called a grease payment, expediting fee, a tip, or envelope, they are often disguised as some type of exchange. Nigerian police personnel may ask for a "little something for the weekend," or a bribe to a border guard may be placed inside the passport. Since proving intent to exchange one favor for another is necessary to convict, a universal rule is to never hand over the cash or check at the same moment of the lobbying attempt. Wait until later.[46]

According to *The Economist*, by giving people power and discretion, whether border guard or grand viziers, some will use their position to enrich themselves. They cite a study that shows that bribes account for eight percent of the total costs of operating a business in Uganda, and corruption boosts the price of hospital supplies in Buenos Aires by 15 percent.[47]

Ernst & Young's 12th Global Fraud Survey entitles "Growing Beyond: A Place for Integrity" found that bribery and corruption is pervasive. For example, in Brazil, 84 percent responded that corruption was widespread. Overall, 39 percent of the respondents said that bribery and corruption practices occur frequently in their countries.

Since CFOs have a significant impact on the payment of bribes, E&Y provided the responses of nearly 400 CFOs to these actions to help their business survive.

- Entertainment to win/retain business 34%
- Cash payments to win/retain business 15%
- Personal gift to win/retain business 20%
- Misstating company's financial performance 4%

As examples, in Indonesia 60 percent of respondents considered making cash payments to win new business acceptable. In Vietnam, 36 percent of the respondents considered it acceptable to misstate their company's financial performance.

In Germany, a sales director once bragged at an office party about how he had bribed several large retail customers. Some only responded to large gifts, he said, recalling one situation when he discreetly pushed a car key to the other side of the negotiating table. The trick was to find out what they liked.[48]

One of his employees commented that what was disturbing about his remarks was the way he bragged about it. In that company, as in countless others, bribery was not only tolerated, it was cool. If a person wanted to become a successful marketing executive, this behavior was what was expected.[49]

What follows is a potpourri of bribe schemes around the world, even at the highest levels of government:

- City Council member Monica Conyers, wife of Michigan congressman John Conyers, plead guilty of accepting cash bribes in exchange for supporting a sludge contract with a Houston company. She received cash envelopes in parking lots of a Detroit community center and a McDonalds.
- In March 2007, a Brazilian federal congressman and former governor of Sao Paulo was charged in New York for stealing more than $11.5 million from a Brazilian public works project in a construction kickback scheme. He allegedly transferred the money to a New York bank and then to an offshore account. The scheme involved inflated and false invoices to contractors involved in the building of a giant highway.
- Two prominent Baton Rouge restaurateurs and four other businessmen were accused of bribing a parish tax auditor and an undercover FBI agent with cash, diamonds, trips, whiskey, and women to avoid paying taxes on $10 million. An indictment alleges Laymon offered an undercover FBI agent posing as an East Baton Rouge Parish auditor $800, a weekend trip to Costa Rica, and two prostitutes a day if he concluded that Arzi's didn't owe any sales tax.
- A Greek prosecutor is investigating claims that Siemens Greece paid up to $550 million in bribes to officials at the defense and interior ministries in order to win a security contract for the 2004 Olympic games in Athens. A senior Siemens accountant said bribery was a common practice at Siemens.
- A Paris judge launched an investigation into allegations that Total, a French oil and gas group, paid bribes to win a $2 billion gas contract in Iran. The investigation stems from the discovery of $82 million in two Swiss bank accounts, allegedly by Total to an Iranian intermediary to help the French company consortium to win an Iranian contract.
- A report claims that AWB, the company responsible for selling Australia wheat, paid over $221 million to Alia, a Jordanian hauling company, ostensibly to distribute its wheat in Iraq. In fact, the money was going to the Iraq government.
- Armstrong Williams, an American columnist and television host, was paid $240,000 by the Department of Education to comment regularly on "No Child Left Behind," an education-reform bill.
- Nineteen individuals were indicted for receiving bribes and rigging bids for school window washing contracts in New York State.
- Congressman Randy Cunningham, R-Calif., resigned from Congress in 2005, hours after pleading guilty to taking at least $2.4 million in bribes to help friends and campaign contributors win defense contracts. Prosecutors said he received cash, cars, rugs, antiques, furniture, yacht club dues, moving expenses, and vacations from four co-conspirators in exchange for aid in winning defense contracts.
- In January 2007, Peter Hartz, former Volkswagen executive, was given a two-year suspended prison sentence and fines for bribing the head of the labor union ($3.25 million) for secret bonuses and fake consultancy fees. The bribe involved sex holidays and paying for prostitutes for German labor officials.

Looking for a paper trail through a series legal documents is unlikely to yield any clues about who was involved in setting up the shell company only a search of electronic communications can yield useful results. Many times the relationship between shell companies stretch around the world as in one recent drug laundering case the money trail ranged from New Zealand to Latvia to Mexico to Wachovia in the U.S. through correspondent banks. All these organizations were involved in laundering money for the Sanaloa drug cartel, and eventually Wachovia paid a fine of $160M for being involved in laundering $420 billion.

Shell companies can be easily set up by fictitious persons. A recent study showed that the international rules and regulations over requiring proof of identity to set up a shell company are largely ineffective.[7] For a fee, incorporation service companies in various countries provide all the legal work that is needed to incorporate a shell corporation. U.S. incorporation services located in Delaware and Nevada were found to be the least interested in securing proper identification from parties incorporating shell companies. The study was based on 7,400 emails sent to more than 3,700 corporate incorporation services that make and sell shell companies in 182 countries.

EXAMPLE 7.8 A money launderer wants to set up an online business to launder monies that are already in accounts held in two offshore banks. These offshore banks are in the Cayman Islands and Nauru, two countries having strong bank secrecy laws.

The launderer sets up a web business located on a web server in the United States. A legitimate Internet service provider (ISP) is used to establish the online business. The business accepts credit card orders. The offshore money has been distributed among a number of bank accounts in the two island banks. These accounts have legitimate credit or debit cards issued with them. These bank accounts, controlled by the money launderer, are used to purchase consulting services from the web company, and the web company invoices the credit card companies for the fictitious services provided. The credit card company invoices the offshore banks, and the money from the fictitious sales is transferred into a Canadian bank account opened by the money launderer in the locale where the alleged company headquarters is located. All components of the scheme are separated from one another and involve cross-border transfers of financial information. Thus, an audit of one business entity in one country would not normally uncover the scam. The documentation generated by the credit card company and the banks is legitimate, and the cash in the banks is assumed to come from legitimate business transactions.

In Example 7.8, the weakest point in the laundering transaction would be the continual purchase of services from the web business through the same accounts at the same two banks. Concentrating an investigation on these specific transactions would be the most useful way to uncover the scheme. Any ISP would be expected to maintain computer logs of all transactions coming through its web servers. These logs would identify the IP address and access phone number with the ISP subscriber. If the ISP does not maintain these logs, this should immediately raise a red flag about its operations. Even if the web business established its own web server, suspicions would be raised if the business did not keep computer logs. If the logs are available, an auditor should review them to determine if any suspicious activity is occurring at the site. For example, if all the IP numbers and phone numbers for the various clients purchasing services are the same or all coming from the same ISP, an investigator should be suspicious.

Casinos

Money launderers use *casino gambling* as a way to launder money. There are a number of techniques to launder money through a casino. The simplest method is for the money launderer to take cash into the casino. A few small normal bets are placed and afterward

the launderer leaves the casino, redeeming his cash at the cashier's cage. In this way, a legitimate source for the cash can be documented. Such activities are used with casinos based in the United States.

Casinos where Americans bet their money do not have to be based in the United States. Online and offshore casinos can be based in any country or in several countries. Another way to legitimize money received in criminal activities is through online gambling. Such gambling has been prosecuted under the Federal Wire Act which was passed in 1961 to control organized crime activities and betting activities where wire communication was used. More recently, Internet gambling in Internet casinos have come under question with the Congressional passage of the Unlawful Internet Gambling Enforcement Act of 2006 ("Act"). The Act illegalized payment processing for Internet gambling operations. Under the law, it is illegal for a bank or financial institution to engage in transferring money to an online gambling website. Prior to the passage of the Act, large amounts of money could be transferred to accounts at businesses that operated Internet gambling websites. Transfers from these accounts to other nongambling accounts would legitimize the money flows. The effectiveness of the law is in question because it has been found to violate World Trade Organization commercial service accords. The E.U.'s European Commission has declared the law protectionist and a violation of E.U.-U.S. free trade guidelines, and many online U.S. gamblers have simply jumped to online services such as UseMyBank (based in Canada) and just continued to gamble with no problems. Due to the nature of the Internet, the Act is largely unenforceable. It is likely that Congress will change the legislation to regulate online gambling in the U.S. rather than outlaw the practices. Many states in the U.S. are seeking other sources of revenue and are considering legalizing online gambling.

SUSPICIOUS ACTIVITY REPORTING REQUIREMENTS. Nevada casinos and tribal governments have been filing FinCEN Form 102, Suspicious Activity Report by Casinos and Card Clubs (SARC), with FinCEN to report potentially suspicious transactions and activities that may occur by, at, or through a casino. Of course, it may be difficult for the casino to identify an individual and file an SARC if they do not have account numbers from credit cards, playing card numbers, or checking accounts. Using cash to buy chips and not using a player's card should circumvent the casino reporting system.

Purchasing Departments

Even normal business purchasing activities can be easily converted into a money laundering operation. By setting up a retail computer company in a country outside the United States, the means are provided for laundering money overseas and back into the United States. Assume that large-scale purchases of computer equipment are made in the United States with money that has been placed in the banking system through *smurfing*. Smurfing is a money laundering technique in which confederates of the money launderer deposit random amounts of less than $10,000 into variously named accounts at a number of different banks. Due diligence procedures such as CTR and SAR filings usually are not triggered by such transactions. Thus, smurfing is most often used to launder smaller amounts of money.

In money laundering schemes involving purchases, the purchased equipment is then sent and sold overseas below cost. A U.S. shell company may be involved. At the point of sale, the money has been legitimized. Once the sales are made, the money can be transferred back through the banking system to the U.S. drug dealer or other criminal as money received from computer sales through export operations. This technique may or may not involve the falsification of invoices below cost to the foreign sales office in order to show a profit on the sale of the equipment.

investigative techniques—often amplified by the application of proprietary technology especially to interrogate large data sets or monitor public sentiment.[10]

EYEWITNESS

Counsel for Omnicom retained Cornerstone Research in a dispute stemming from Omnicom's stock price decline following a 2002 *Wall Street Journal* article. The plaintiffs claimed that the article was a class-period-ending corrective disclosure that revealed allegedly improper accounting for Omnicom's investments in certain interactive advertising companies. The plaintiffs alleged damages in the billions of dollars.[11]

Cornerstone Research supplied three experts, including Professor William Holder of the University of Southern California, for the defendant, Omnicom. Professor Holder reviewed Omnicom's accounting for its investments in interactive advertising companies and concluded that the accounting judgments of Omnicom's management were reasonable. Cornerstone Research also supplied a loss causation expert who examined the role that the article played in Omnicom's stock price decline and an industry expert who discussed typical business practices in venture capital transactions.[12]

The U.S. District Court of Southern New York granted summary judgment in favor of Omnicom, rejecting the claims in their entirety because the plaintiffs had not proven loss causation. The court found that the plaintiffs had failed to "distinguish the alleged fraud from 'the tangle of [other] factors' that affect a stock's price," as required by the Supreme Court's *Dura* ruling.[13]

SPOTLIGHT

THE PAID EXPERT. David Teece was born in New Zealand but moved to the United States in the early 1970s. While working on a Ph.D. at the University of Pennsylvania, he worked on a summer project for $3,000 to help fight price-fixing against Exxon. Today he owns 7.3 percent of LECG, currently valued at $17 million. In 1997, when LECG went public, his faculty members were shocked to see that Dr. Teece was earning $700,000 a year as an expert witness. He does not dispute that his career earnings from expert consulting amount to at least $50 million.[14]

In one case testifying for Philip Morris, much of his testimony was as plain spoken as a tenth-grader in a social-studies class. Philip Morris' executives or lawyers could have said the same, but since Professor Teece was a prominent scholar and independent thinker, his remarks carried extra weight. The jurors ruled in favor of Philip Morris.[15]

However, in a 2001 dispute, District Court judge Robert Payne said that Dr. Teece royalty estimates were "a wild guess." The judge remarked that "I have the impression, from what I have read, that Mr. Teece will say just about anything."[16]

¶ 8006 A DISPUTE BEGINS

John Grisham gives two major ways to sue in the civil courts: (1) by ambush, or (2) serve and volley. With an ambush, the attorney prepares a skeletal framework of the allegations, runs to the courthouse, files the suit, leaks it to the press, and hopes he or she can prove what is alleged. A serve and volley begins with a letter to the defendants, making the same allegations, but rather than suing, the attorney invites a discussion. Letters go back and forth trying to reach a compromise so litigation can be avoided.[17]

There are two different courtroom environments: civil and criminal. Some experts believe it is more difficult to convict in a criminal trial. E.J. McMillan says "you have to remember

one thing, and this is the fact that our laws aren't designed to punish guilty people; they're intended to protect innocent people."[18] And Clinton McKinzie says "I have never come to terms with a system based on the principle that it is better to let hundreds of guilty people go free rather than wrongly convict one innocent person. It's okay for people to be victimized again and again as long as no one is mistakenly locked up."[19] In a civil trial, however, the jurors try to give away as much money as possible, because it is not their money, and there are no guilty feelings. Plaintiffs generally wish a jury trial. Accountants may be used in both civil and criminal situations.

There is now a so-called "CSI effect" because of the three shows on television. Peoria State's attorney Kevin Lyons says that the shows "project the image that all cases are solvable by highly technical science, and if you offer less than that, it is viewed as reasonable doubt. The burden it places on us is overwhelming."[20] Barbara La Wall, the county prosecutor in Tuscon, Arizona, says that jurors expect criminal cases "to be a lot more interesting and a lot more dynamic. It puzzles the heck out of them when it's not."[21]

Winning in a civil trial may only be a pyrrhic victory because the plaintiff may never receive payment of any judgment. For example, O.J. Simpson never paid the $474 million judgment against him. Also, Robert Blake had a $30 million civil judgment against him, but he declared bankruptcy.

EYEWITNESS

A disappointed jury can be a dangerous thing. Just ask Jodi Hoos. Prosecuting a gang member in Peoria, Illinois for raping a teenager in a local park, Hoos told the jury, "You've all seen CSI. Well, this is your CSI moment. We have DNA." Specifically, investigators had matched saliva on the victim's breast to the defendant, who had denied touching her. The jury also had gripping testimony from the victim, an emergency-room nurse, and the responding officers. When the jury came back, however, the verdict was not guilty. Why? Unmoved by the DNA evidence, jurors felt police should have tested "debris" found in the victim to see if it matched soil from the park. "They said they knew from CSI that police could test for that sort of thing," Hoos said. "We had his DNA. We had his denial. It's ridiculous."[22]

The six major phases of litigation are:

- Pleadings
- Discovery
- Pre-trial conferences
- Trial
- Outcome
- Possible appeal

Much of the work for forensic accountants occurs in the discovery stage.
The pleadings consist of:

- *Complaint*—Plaintiff files.
- *Service of process*—Served on defendant.
- *Answer*—Defendant must admit or deny allegations.
- *Demurrer*—No cause of action exists.
- *Possible cross-complaint*—Defendant files.

An attorney's job is to ultimately avoid trial and the resulting lost time and expenses. Thus, the goal of a forensic accountant is to help the attorney to avoid the cost and uncertainty of a trial.[21]