



fraud alert

year end 2004

Occupational fraud still stings

**ACFE "Report to the Nation"
confirms a costly problem**

How HIPAA fights health care fraud

**Hang up on fraud with
confidential hotlines**

**Forensic accountants
assume proactive roles**

**Pumped-up stocks leave
investors in the dumps**

▲
ROGERS, LYNCH & ASSOCIATES LLC

▲
▲

7051 Argonne Blvd. New Orleans, LA 70124 Phone: 504.282-1441 Fax: 504.282-6641 www.rlastars.com

Occupational fraud still stings

ACFE “Report to the Nation” confirms a costly problem

When owners and executives perpetrate fraud, they are most likely to be exposed by tips from employees. The losses caused their companies are 14 times higher than losses caused by employees, but they are less likely to face legal action as a result.

Those are just some of the findings in the *2004 Report to the Nation on Occupational Fraud and Abuse* by the Association of Certified Fraud Examiners (ACFE). To assemble the report, the ACFE surveyed certified fraud examiners who investigated 508 cases totaling more than \$761 million in losses.

Examiners reported that owner and executive fraud is less common than employee fraud (12% compared to 68%) but is significantly more costly. The median loss for owner and executive fraud was \$900,000, compared to \$62,000 for employee fraud. More disturbing, owner and executive fraud is often much more difficult to detect.

Tips vs. internal controls

Like all fraud, owner and executive improprieties most often come to light as the result of an employee tip — evidence of the value of confidential reporting mechanisms. An additional finding emphasizes the importance of making reporting mechanisms available outside the company, as well: About 20% of total tips came from customers, 15% from vendors and 13% from anonymous sources.

In addition to helping identify fraud, confidential reporting mechanisms can also significantly reduce losses once fraud occurs. Organizations that allowed anonymous tips suffered a median loss of \$56,500 — less than half the loss experienced by organizations without these systems.

Tips also were responsible for revealing the largest frauds. Of the 71 cases that involved losses of

\$1 million or more, 43% were revealed by employee tips. (To learn more about confidential reporting mechanisms, see “Hang up on fraud with confidential hotlines” on page 5.)

Those findings support the Sarbanes-Oxley Act’s requirement that publicly traded companies establish anonymous reporting mechanisms for employees. They offer less justification for the act’s heavy reliance on internal controls to detect fraud. Internal controls were fourth on the list of methods that detected fraud in the surveyed cases — behind accidental discovery, which was third.

The report adds, however, that the findings should not be construed to mean that internal controls should be abandoned. Rather, they should serve

What does a fraud perpetrator look like?

Men and women are roughly equal when it comes to the number of frauds they commit, but men’s fraudulent schemes result in significantly higher losses — \$160,000 compared to \$60,000 for women. That may be because men tend to occupy positions of greater authority, according to the Association of Certified Fraud Examiners’ *2004 Report to the Nation on Occupational Fraud and Abuse*.

Other report findings on fraud perpetrators include:

- Nearly half of frauds are committed by people older than 40,
- Fewer than 20% of perpetrators are younger than 30,
- Two-thirds of fraud perpetrators act alone,
- When fraud is a result of collusion between two or more employees, the median loss soars from \$58,500 to \$200,000,
- Most perpetrators have no previous criminal record, and
- Losses from fraud increase the longer someone has been on the job. Fraud by employees who have been employed 10 or more years has a median loss of \$171,000. For those who have been with a company one or two years, the median loss is only \$50,000.

as wake-up calls to alert businesses to the need for more effective internal antifraud controls.

Fraud is costly

Determining the true cost of occupational fraud is virtually impossible, in part because many frauds go undetected, unreported or unprosecuted. Survey respondents estimated, however, that a typical organization loses 6% of its annual revenue to fraud. If accurate, those estimates would translate to \$660 billion a year, based on the 2003 U.S. gross domestic product.


Small businesses — those with fewer than 100 employees — suffer disproportionately. The study found they were targets in 46% of the cases, and suffered a median loss of \$98,000. Only companies with more than 10,000 employees (which accounted for only 13% of fraud cases) suffered greater losses, with a median of \$105,500.

Prevention programs

Overall, the ACFE's report held few surprises, but reaffirmed the need for every business to establish comprehensive and effective programs to combat



fraud. Sadly, businesses attacked by fraud are unlikely to recover their losses. The median recovery is 20% of the loss, and about 40% of victims recover nothing at all.

The most cost-effective means of dealing with fraud is to keep it from happening. If your company has yet to implement a fraud-prevention program, forensic accountants can help you develop one. 

How HIPAA fights health care fraud

Much has been written about the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA). But companies may also want to pay some attention to provisions that have received less attention, namely, the new penalties for health care fraud. These HIPAA regulations are significant and could help take a bite out of the country's serious health care fraud crisis.

Criminal offenses with big penalties

HIPAA defines four new federal criminal offenses specific to health care:

- **Health care fraud.** Any attempt to defraud a health care benefit program or fraudulently obtain program benefits.
- **Theft or embezzlement in connection with health care.** Stealing, embezzling or misapplying any assets of a health care benefit program.

- **Making false health-care-related statements.** Concealing or falsifying facts or making false or fraudulent statements.
- **Obstruction of criminal investigation of health care offenses.** Attempting to prevent, delay or otherwise impede communication to a criminal investigator.

With penalties of as much as 10 years in prison and fines of up to \$250,000 per offense, HIPAA carries some significant muscle. If a patient is injured as a result of fraud, the prison term is doubled; if the patient dies, a perpetrator can be sentenced to life in a federal prison.

Many states have also strengthened their health care fraud statutes. But according to various estimates, health care fraud still accounts for \$40 billion to \$130 billion in losses every year.



Although the vast majority of health care providers are honest and ethical, the fraudulent few are significantly affecting government and private benefit providers and driving up the cost of obtaining coverage for the average person.

Unfortunately, consumers aren't always blameless, either. Consumers may file false claims, alter bills or receipts or use someone else's coverage to obtain benefits — actions that all contribute to an increase in health care fraud.

Congress isn't the only entity determined to stop health care fraud. The Blue Cross and Blue Shield Association announced in April 2004 that it has formed an antifraud strike force to work with the FBI and other law enforcement agencies. In addition, the association established a consumer hotline and Web site to encourage reporting of suspected fraud.

The many faces of fraud

By far the greatest damage is done by dishonest providers, according to the National Health Care Anti-Fraud Association (NHCAA), a not-for-profit organization based in Washington, D.C.

Fraudsters take advantage of the sheer size of the U.S. health care industry in a number of ways. They may bill for services they never perform, falsify a patient's diagnosis to justify unnecessary tests and procedures, bill each stage of a procedure as if it were a separate procedure, accept kickbacks for patient referrals or bill patients for services that managed care programs have already paid.

Fraudulent providers can also bill many different payors for the same treatment, hoping their fraud will go undetected among the more than four billion health insurance claims that the NHCAA says are processed every year in the United States.

Identifying culprits

Because there are so many ways providers can defraud the system, Congress established the Health Care Fraud and Abuse Data Collection Program to ensure that government agencies and health plans have access to information on fraudulent providers.

The database contains reports of all adverse actions (other than malpractice claims or settlements made with no finding of liability) taken against health care professionals, providers and suppliers. This can alert benefit plans and other payors to be wary of those individuals and organizations.

Fraud fight scores victories

Clearly, antifraud efforts are having some effect. In March, the FBI raided three outpatient-surgery clinics in Southern California, ending a scam that bilked insurers and employers out of up to \$500 million over a period of several years.

Other recent victories include the arrests of a Boston psychiatrist who reaped at least \$1.3 million in payments for phony treatments and a Chicago cardiologist charged with performing unnecessary procedures over a 10-year period.

Still, the government's recovery of \$5.7 billion from civil fraud actions between 1999 and 2003 is a rather small drop in a very large bucket. And, while health care fraud is expensive, more than money is at stake. False diagnoses or treatments mean false patient records — records that may only come to light during medical emergencies. Worse, some patients are put at physical risk by unnecessary medical tests and procedures.

HIPAA helps

Health care fraud affects everyone and is too dangerous and costly to be overlooked. Identifying fraud requires a joint effort by law enforcement agencies, health plan providers and consumers. With HIPAA, Congress has established more significant options for punishing the perpetrators in a serious effort to get health care fraud under control. ¶

Hang up on fraud with confidential hotlines

Tips from employees are the first and best line of defense any company has against fraud. Unfortunately, fear of retribution and concern about being labeled a “whistleblower” may make employees turn a blind eye to fraud or financial irregularities.

That silence can be expensive. A typical U.S. company loses 6% of its annual revenue to fraud, according to the Association of Certified Fraud Examiners (ACFE). When employees are willing and able to report suspicious activities, however, the loss can be cut in half.

Studies show the best way to encourage employee tips is through a confidential, 24-hour hotline operated by a third party. The 2002 Sarbanes-Oxley Act requires publicly traded companies to make some such anonymous mechanism available, with stiff penalties for noncompliance. For private firms, an internally operated hotline can also be successful — if it is run properly.

Make reporting comfortable

The first step is to let employees know that it’s all right to report irregularities and that they will remain anonymous when they do. They also need detailed written guidelines about what constitutes acceptable behavior and how they can recognize fraud.

Reinforce these messages by repeating them periodically in different venues. For example, you can follow the original communication with paycheck enclosures, cafeteria displays, newsletter articles or postings on your company’s intranet.

Regardless of how the message is delivered, it must be specific. Don’t encourage people to report “accounting irregularities” or “fraudulent actions.” Tell them what constitutes fraud, and then tell them how to report it.

In a company with hundreds or thousands of employees, for example, an anonymous message saying, “My manager is stealing a lot of money from the company,” is unlikely to be of much value.

To guard against receiving such confusing tips, hire a trained interviewer to answer all hotline calls. An experienced interviewer can get enough additional details from anonymous callers to be able

to properly focus an investigation. Also remember that employees aren’t likely to call hotlines from their desks, so the hotline must be staffed around the clock, seven days a week.

Follow up matters


A common deterrent to fraud reporting is the perception that nothing happens when reports are made. Fully one-third of employees who call anonymous hotlines do so only after they have already reported their suspicions to managers who ignore or white-wash the complaints, the ACFE says. To make a hotline valuable as a fraud deterrent, you need to take every tip seriously and investigate every allegation.



You also need to make sure that the results of this scrutiny go to the right people, even if the hotline is used for something other than fraud. Employees may use a hotline for discrimination, sexual harassment or other nonfinancial but potentially litigious complaints. Your report dissemination procedure, therefore, must ensure that all tips are routed to the proper departments.

Finally, don’t limit hotline access to employees. Make it available to suppliers, customers and investors — all of whom may be privy to kinds of activities different from those seen by employees. The more people who can access the line, the more likely it is to help shut down all avenues of fraud.

Hotlines help

Ethics hotlines won’t replace established fraud-detection procedures such as internal and external audits and employee reports to management. They may, however, serve as early-warning systems that can avert lawsuits and headlines as well as reduce fraud. 

Forensic accountants assume proactive roles

It's one thing to recognize fraud when you see it. It's another to identify opportunities for fraud before anyone exploits them — but that's just what forensic accountants do.

As companies survey the financial rubble of recent high-profile corporate collapses, many are calling on forensic accountants not only to track down and eradicate fraud, but also to prevent it. Indeed, forensic accounting is one of the fastest-growing areas in the accounting industry.

Traditional role expands

Traditionally, forensic accountants have been called in only when an auditor, whistleblower or other source raises a red flag. Forensic accountants have been extremely effective in tracking down financial crime, but their role has largely been reactive. They are summoned in response to suspicion — or outright theft.

That may be changing as corporate boards explore every avenue to avoid becoming the next financial scandal. Some directors contend forensic accountants should be called to do regular overall checkups on corporate books; others believe forensic accountants should focus on specific areas of financial statements.

Either way, there is growing agreement that the role of forensic accountants should expand to encompass prevention as well as detection.

Traditionally, forensic accountants have been called in only when an auditor, whistleblower or other source raises a red flag.

Getting past the basics

For one thing, proponents say, regular auditors and forensic accountants use different approaches in their jobs. Regular auditors focus on errors, omissions, exaggerations and misstatements. Forensic accountants, or fraud auditors, on the other hand, concentrate on exceptions, irregularities and patterns.

The sheer volume of records that is included in a regular audit requires auditors to use something similar to a random sampling to complete their jobs. If that sampling doesn't uncover fraud warning signs, regular auditors won't detect it.

By contrast, forensic accountants zero in on the types of accounts where fraud is most likely to occur: payables, payroll, benefits, expense claims, sales revenue, inventory, profits and deferred expenses. Not only can they identify opportunities for fraud, they also will follow the trail of any suspicious activity to its bitter — or benign — end.


Now's the time

There is nearly universal agreement that it is time for forensic accountants to assume more proactive positions in the corporate financial realm, but it remains to be determined how that will be accomplished.

Some accounting firms are adding forensic specialists to their regular audit teams to help boost clients' comfort levels. In other cases, companies prefer to



bring in their own third-party examiners for guidance when their internal and external auditors are at odds. Another option is to have forensic accountants supervise external auditors' work to be sure no impropriety is left unexposed.

Of course, even the closest scrutiny won't catch all fraud — particularly if a firm's top management is colluding to perpetuate it. Forensic accountants can, however, make it significantly more difficult for frauds to succeed. 



Fraud to watch for: **Pumped-up stocks leave investors in the dumps**

First, buy shares of a worthless stock few people have heard of. Then, tout the company on the Internet and wait for others to buy and artificially inflate the stock's price. Finally, sell your shares for a tidy profit.

It's easy to get caught when you attempt this classic "pump and dump" scheme, but many fraudsters find the possibility of making a lot of money in a very short time irresistible enough to try it.

According to the Securities and Exchange Commission, there have been thousands of cases of pump and dump fraud in recent years. One of the most notorious involved a 15-year-old New Jersey boy who was ordered to repay \$272,826 plus interest, after his scheme was uncovered.

But that was small potatoes compared to the amount one New York organized crime ring was charged with swindling from investors in 2001. The 20 men charged ran their pump and dump scheme through three brokerage houses, bilking investors — including several well-known professional athletes — out of \$50 million.

One scam fits all

Regardless of their scope, however, pump and dump scams all operate in basically the same way. The perpetrators buy cheap stock in thinly traded companies that have tight floats. (Most shares are held by insiders and promoters, rather than the general public.)

They then promote the stock online through e-mails, message boards and chat rooms.

Often, the promotions will claim to be from day traders, insiders or other knowledgeable people. They may include "tips," such as a \$2 stock will soon sell for \$20, or grandiose claims urging investors to buy now and their shares will increase 1,000%. The promotions all attempt to convince investors they can get rich quickly because they have information that isn't widely known.

In some cases, the perpetrators themselves will quietly buy more shares to help drive the price up. Most often, they simply wait for unsuspecting marks to do it for them. Since the stock isn't widely traded, it doesn't take too much activity to send the price soaring.

When the price gets high enough, the fraudsters sell their own stock as the innocent buying continues. That "dump," coupled with an immediate end to the bogus promotions, deflates the price, which declines even further as panicked buyers sell in an effort to minimize their losses.

Let the buyer beware

To combat pump and dump, as well as other Internet fraud, the Department of Justice has two interagency initiatives, the Internet Fraud Initiative and the Internet Fraud Complaint Center. Both are dedicated to disseminating information and training regulatory personnel, as well as accepting and pursuing tips.

When caught, pump and dump perpetrators rarely go unpunished, but the scheme continues to be popular. To avoid getting snared, be extremely wary of unsolicited online messages or grandiose claims about any stock. The bottom line: If you're considering a great stock buy, consult a reputable broker.

Don't Let Fraud Ruin Your Business

Occupational fraud and abuse costs American businesses an estimated \$600 billion annually — roughly \$4,500 per employee. Small businesses are the most vulnerable to these crimes. But you don't just have to stand there and be victimized by them.

Let Rogers, Lynch & Associates LLC assist you in combating fraud and abuse. We offer a wide range of forensic accounting, and fraud-related services, including:

- Litigation Consulting and Support
- Expert (Witness) Services
- Fraud Detection and Deterrence
- Insurance Claim Analysis: Loss Profits, Business Interruption, Surety Bond Claims, Fidelity Bond Claims
- Divorce/Community property Partition
- Evaluation of Internal Control Systems
- Financial Statement Analysis and Interpretation
- Bankruptcy and Reorganization
- Asset Recovery
- Track and Locate Assets Misappropriated

Since our firm's founding in 1989, we have been committed to providing our clients professional service of the highest quality. Our clientele includes family and closely held businesses, public corporations, and commercial lenders throughout the United States.

We would welcome the opportunity to help you prevent, detect, or prosecute fraud. Please call us at 504-282-1441 or visit our Web site: www.rlastars.com, and let us know how we can be of assistance.



Patrick M. Lynch, CPA, CFE, DABFA, CrFA, CPCU, CLU, AIC

Managing member has over 30 years experience in fraud detection and deterrence and has testified as an expert witness in US Bankruptcy Court.



Penny Rogers Baumer, CFE, DABFA

Managing member has over 20 years experience in fraud detection and deterrence and has testified as an expert witness in US Bankruptcy Court.

Rogers, Lynch & Associates LLC
Certified Public Accountants • Certified Fraud Examiners
Certified Forensic Accountants • Business Consultants
7051 Argonne Blvd. New Orleans, LA 70124
504-282-1441
www.rlastars.com