Forensic Focus

Insights on fraud detection and deterrence

YEAR END 2008

ACFE Report
Businesses bear the brunt of rising fraud costs

Don't shortchange your business with under-the-table wages

Taking a bite out of health care fraud

Realistic fakes: A new challenge for insurers

Are your managers riding roughshod over internal controls?

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

105 W. Madison Street • Suite 406 • Chicago, IL 60602
www.mcgoverngreene.com

ACFE Report

Businesses bear the brunt of rising fraud costs

The cost of fraud is going up, and small businesses continue to shoulder a disproportionate share of the load, according to the 2008 *Report to the Nation on Occupational Fraud & Abuse* by the Association of Certified Fraud Examiners (ACFE). Small businesses (defined as having fewer than 100 employees) experienced the largest median loss: $200,000.

Industrial strength

The latest version of the biennial ACFE report estimates that U.S. businesses lose 7% of their annual revenues, or $994 billion total, to fraud. That's a sizable increase from the estimated 5%, or $652 billion, in fraud losses reported in the 2006 survey.

Losses in some industries outpace those in others. Manufacturing, for example, reported the largest median loss, at $441,000, followed by banking ($250,000) and insurance ($216,000). The most common casualties of fraud, however, were banking and financial services, which accounted for 15% of reported cases. Government (12%) and health care (8%) were also frequent victims.

More striking than the differences among industries were those according to type of organization. Private companies, which comprised nearly 40% of respondents, sustained a median loss of $278,000 in 2008, compared to $210,000 in 2006. Public companies, however, reported a median loss of only $142,000 in 2008, down 29% from the $200,000 median loss public companies reported in 2006.

SOX helps

The ACFE attributes significantly reduced fraud among public companies in large part to reforms mandated by the Sarbanes-Oxley Act of 2002 (SOX). Public companies that were using SOX-mandated controls experienced median losses that were from 70% to 96% lower than those reported by companies that had not yet implemented SOX controls.

SOX stipulations also appear to help companies identify fraud sooner — with one exception. Management certification of financial statements, which resulted in a 96% reduction in fraud losses, did nothing to speed discovery of fraud in public companies. In fact, companies that implemented management certification reported a 20% increase in the number of months to detection.

In private companies, however, management certification of financial statements reduced

The who and how of it

According to the 2008 ACFE *Report to the Nation on Occupational Fraud & Abuse*, nearly a third of the fraud reported between 2006 and 2008 originated in accounting departments, and 18% of schemes were attributed to executives or upper management. When upper managers were involved, the median loss soared to $853,000, making these the costliest frauds reported.

Approximately nine out of 10 fraud perpetrators were first-time offenders, making it nearly impossible to identify them through controls such as background checks. More useful, the report says, were behavioral red flags. Nearly 40% of fraud perpetrators were living beyond their means, and 34% were experiencing financial difficulties at the time of the fraud.

Most fraudsters had been with their companies from one to five years, but the median loss was greatest when perpetrators had been employed from six to 10 years — $261,000 compared to $142,000.

detection time by 25%. The study's results suggest that private companies that have yet to adopt SOX are well advised to do so.

Difference between big and small

Across all industries and types of organizations, fraud schemes in small businesses differed somewhat from those prevalent in larger companies. Small businesses were much more likely to fall victim to check-tampering and billing fraud. In fact, nearly 29% of small business fraud involved billing schemes, and check tampering was cited in more than 25% of small business cases, compared to about 24% and 15%, respectively, in larger companies.

The study's results suggest that private companies that have yet to adopt SOX are well advised to do so.

Inadequate segregation of duties — common in smaller companies with fewer employees — in cash disbursement functions often contributes to check tampering. Small businesses, however, are somewhat less likely to experience purchase and sales scams or corruption schemes such as kickbacks, bid rigging and extortion than their bigger counterparts.

Damage controls

Internal controls can't prevent every fraud incident, but the report demonstrates that controls are effective in mitigating damages when fraud occurs. Organizations with controls in place reported significantly lower losses than those without them. Indeed, lack of internal controls was the most-cited reason that fraud occurred, with 35% of organizations saying it was a contributing factor.

Ironically, the two controls associated with the largest reductions in fraud losses were among the least likely to be used. Only about 25% of reporting organizations were using surprise audits when fraud occurred, but their losses were 66% lower than the median losses experienced by businesses that didn't use surprise audits.

And companies that rotate jobs and have mandatory vacations lost 61% less than companies that didn't have these controls. Yet only about 12% of companies included job rotation and mandatory vacation in their fraud control procedures.

Other controls that proved highly effective in reducing median losses included:

- Anonymous hotlines,
- Employee support programs,
- Management fraud training,
- Employee fraud training, and
- Regular internal audits.

All were credited with loss reductions of at least 50%, compared to companies that didn't use them. On the other hand, rewards for whistleblowers, management certification of financial statements and independent audit committees were rated among the least effective controls.

Picking up the pace

The 2008 ACFE report concludes that fraud continues to thrive and grow in the United States. Therefore, businesses that don't yet have robust fraud control programs need to implement them. And companies with controls should examine them for effectiveness. As the report illustrates, the cost of ignoring fraud is getting higher. ■

Don't shortchange your business with under-the-table wages

Business owners are always looking for ways to improve their financial position, and some may be tempted to pay workers in cash. If you've considered it, resist the temptation. Not only do you and your employees risk penalties, but under-the-table wages may do significant financial damage to your business.

Risky business

Employers typically make financial justifications for paying cash wages: It lowers tax and insurance costs, reduces bookkeeping time, and can provide them with a competitive advantage. Sometimes, they argue, employees ask to be paid in cash, and cash wages are routine in some industries, such as restaurants and construction.

Even if all that were true, it doesn't matter. To avoid possible legal repercussions, you must withhold taxes from your employees' pay. You can, of course, pay employees in cash if you prefer. But you need to report what you pay and deduct the appropriate taxes and pay the employer portions of Social Security and Medicare, and a percentage in unemployment insurance.

Paying the piper

The withholding process may be complicated, but it can save you money in the long run. Consider the case of a Massachusetts man who, in an effort to avoid paying payroll taxes and reduce unemployment insurance premiums, paid more than $43 million in under-the-table cash wages to temporary agency laborers. The man was sentenced in July 2008 to nine years in prison and ordered to pay more than $12 million in restitution.

Even if you're caught paying undocumented wages on a much smaller scale than that business owner, the IRS will likely be interested in you. It has broad powers to go after employers who don't withhold taxes from employees' paychecks, and violators can be liable for as much as 100% of the taxes they should have paid, plus interest and penalties. And that's just on federal taxes; you'll still owe state and local taxes and unemployment premiums, along with associated interest and penalties.

Employees share the blame

You aren't the only one at risk, either. If other people in the company share responsibility for payroll tax deductions, they can face the same penalties as the owner. For example, if you and two senior executives are deemed responsible parties for $15,000 in taxes that weren't withheld, the IRS potentially could collect a total of $45,000, plus interest and penalties.

Under-the-table wages can have another cost — time. If regulators find unreported wages during an audit of your business, you'll be required to reconstruct your payroll records going back at least to the time you stopped reporting wages. If officials suspect you were intentionally breaking the law, they can keep going back further, potentially all the way to your company's inception.

Employees who receive unreported wages share the blame. They're subject to tax audits for not reporting their wages and are liable for any subsequent penalties. And these workers have no paycheck stubs or W-2 forms to verify their wages, which could make getting a bank loan or lease difficult. Worse, the employees aren't accruing Social Security benefits and could be denied unemployment compensation if they lose their jobs.

Avoid shortcuts

Under-the-table wages may seem like a good deal both for your balance sheet and your employees' pocketbooks, but the practice comes at a high cost. If you don't want to pay that cost, don't take the risk. ■

Taking a bite out of health care fraud

For every dollar the federal government spent investigating whistleblower-reported health care fraud in 2007, it recovered $15, according to Taxpayers Against Fraud. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) can take much of the credit for this success.

Rooted in history

HIPAA's fraud and abuse provisions can be traced as far back as the Civil War, when the False Claims Act was enacted to protect the Union army from fraudulent suppliers. More than a century later, Congress approved HIPAA, broadening the False Claims Act to make health care fraud a separate offense and, more important, creating a source of revenue to combat it.

The vast majority of health care fraud in the United States is perpetrated by a small number of providers.

The National Health Care Anti-Fraud Association says fraud now consumes as much as 10% of the nation's annual $2.26 trillion health care outlay. That translates into higher insurance premiums for individuals and employers, and adds to the cost of doing business. What's more, fraudulent medical records may jeopardize patients' health by misrepresenting actual medical conditions.

A few bad apples

The vast majority of health care fraud in the United States is perpetrated by a small number of providers — but it spans the spectrum of care. The Department of Justice has taken action against individual physicians, hospitals, pharmaceutical manufacturers, nursing home networks, pharmacies and durable medical equipment suppliers.

The most common types of health care fraud are:

- Billing for services that weren't provided,
- Upcoding, or billing for more expensive services than the ones provided,
- Providing unnecessary services,
- Falsifying diagnoses to justify unnecessary tests or surgeries,
- Billing every step of a procedure as a separate procedure,
- Billing patients more than copay amounts for services paid in full by managed care providers,
- Waiving patient copays and overbilling payors, and
- Accepting kickbacks for referrals.

Not only do such schemes add to everyone's health care costs, but they also eat into patients' lifetime benefits caps. Every false dollar spent adds to patients' totals, meaning they may not have the resources to combat a major medical condition.

Money talks

Thanks to HIPAA, the fight against fraud is easier to wage. Before HIPAA, health care fraud primarily was prosecuted as mail fraud or making a false statement to Medicare, with a maximum penalty of a significant fine and as much as five years in prison.

Under HIPAA, health care fraud is punishable by life in prison if someone dies as a result of the fraud. The penalty for less serious cases is a substantial fine — triple the overcharged amount and up to $10,000 per violation — and up to 10 years in prison. HIPAA also established ongoing funding for the Department of Justice, FBI, and Department of Health and Human Services to investigate health care fraud. And it has redefined health care fraud to broaden enforcement capabilities.

Health care fraud no longer must be intentional to be pursued in civil court. Instead, if someone should have known activities were fraudulent, that individual is subject to civil action. In addition, HIPAA increased incentive payments available to whistleblowers and allowed federal agencies to contract investigations out to private firms.

The fight continues

HIPAA is only 12 years old, but already it's demonstrating its worth. Health care fraud cases now outpace military false claims cases as the largest source of financial recoveries, according to BNA, a leading health news publisher. As encouraging as the news is, more fraud needs to be caught. Fortunately, HIPAA is making the job a little easier. ■

Realistic fakes: A new challenge for insurers

After a woman's home was burglarized, she gave her insurance company receipts to support her claim that more than $5,000 in property had been stolen. There was just one problem: The receipts were fake.

Thanks to the newest Internet entrepreneurs, this type of incident is becoming all too common. Web sites proudly proclaim they can produce receipts from any store in the world, in any amount, and for any product. All you have to do is ask — and pay about $30.

The fake receipt sites purport to be intended for gag gifts or to help straying spouses cover up their activities. They may even post a disclaimer warning buyers that fake receipts shouldn't be used for fraudulent purposes. But they make no attempt to police what people do with the receipts they order.

As a result, those bent on insurance fraud have a new weapon in their arsenals. But insurers are becoming better at spotting fake receipts, and legal authorities are very willing to prosecute those who use them.

Law enforcement officials in Louisiana, New Hampshire and New Jersey, to name just a few states, have prosecuted offenders for using false sales receipts to defraud insurance carriers. In a California case, perpetrators worked with store employees to file fictitious property theft claims. More often, however, these schemes involve individual homeowners who inflate claims after fires or burglaries.

Penalties can be severe. Convicted fraudsters face fines that can reach into the hundreds of thousands of dollars and prison sentences that can extend to 20 years or more.

Most insurance companies have quickly gotten smart about realistic-looking, but fake, receipts and they verify the authenticity of support documents submitted with loss claims. Those insurers that don't, however, face a significant new area of risk.

Are your managers riding roughshod over internal controls?

Certified Fraud Examiners have cited management override of internal controls as the primary facilitator of fraud in 17% of the cases they've investigated between 2006 and 2008. Most of those frauds were uncovered only because an employee or other source brought them to light.

It may be difficult to believe, but as these findings from the 2008 ACFE *Report to the Nation on Occupational Fraud & Abuse* show, anyone is capable of committing fraud — even trusted managers. You don't want to think it could happen, but need to protect against it just the same.

Managers feel the pain

Fictitious or premature revenue recognition, overstated assets, and understated expenses or liabilities are among the most common types of management fraud. Managers can, by overriding internal controls designed to detect fraud, record nonexistent or improper sales, undervalue bad debt allowances or inventory reserves, or simply not accrue liabilities.

Your managers, of course, must have some flexibility to override financial reporting internal controls. However, these should be rare occurrences, and your company should require the employee to obtain subsequent approval from you or another authorized manager. Unusual and unsupported entries made to these accounts should raise red flags.

Besides unusual entries that may suggest managers are taking advantage of their override privileges, look for unexpected activity in financial records. If an account is posted through a journal entry, rather than as a normal transaction, dig a little deeper to learn why. Similarly, if transactions are initiated by unexpected parties, or adjustments made without required approvals, get to the bottom of them.

Such activities aren't definitive indications of fraud, but they are warning signs. If nothing else, they signal a need to overhaul your accepted accounting procedures before a thief finds a way to manipulate your current system.

Avoiding unrealistic goals

Even trusted managers are subject to the same "fraud triangle" of influences that cause rank-and-file employees to commit fraud: incentives or pressure, opportunity, and rationalization. Managers also may feel pressured to meet your company's challenging financial performance targets. So in examining the strength of your fraud control procedures, consider whether your managers' performance goals are realistic.

Despite your best efforts, management fraud can still be difficult to anticipate and detect. The 2008 *Report to the Nation* notes that frauds by managers and owners last twice as long as those perpetrated by lower-level employees. That may be in part because managers intimidate their subordinates into silence.

Still, the people just below managers often are the first to know that something is amiss. To help combat managerial fraud, cultivate a comfortable relationship with employees a level or two lower than your managers.

Raise your standards

You trust your managers and don't want to alienate them or feel compelled to monitor their every move. But that doesn't mean you should take everything they say at face value, or that you don't need to understand and test your financial reporting and accounting processes. ■

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

SPECIALISTS IN FRAUD EXAMINATION AND LITIGATION SERVICES

If a business hasn't yet been a victim of fraud, it's been fortunate. According to the Association of Certified Fraud Examiners, fraud costs businesses in the United States billions of dollars every year. Small businesses are especially vulnerable because they often do not have controls in place to reduce the likelihood of fraud.

This is where McGovern & Greene LLP can help. Our firm specializes in helping corporations, attorneys, lenders, law enforcement and governmental agencies analyze financial records and contracts, identify and prevent fraud, recover and analyze evidence, and provide expert testimony in all of these matters. Our highly-experienced team of professionals includes certified fraud examiners and certified public accountants who are experts in the fields of fraud examination, forensic accounting, computer forensics, damage calculations, business valuations and audit services.

Our professionals can assist you in a wide range of matters, including:

- **Fraud Examination**
- **Due Diligence**
- **Training & Seminars**
- **Electronic Discovery**
- **Financial Investigations**
- **Business Valuation**
- **Profit Recovery**
- **Government Contracts**
- **Contract Claims**
- **Forensic Accounting**
- **Asset Recovery**
- **Litigation Services**
- **Economic Damages**
- **Construction Audits**
- **Computer Forensics**
- **Internal Audit Services**
- **Healthcare Audit**
- **Intellectual Property**

CRAIG L. GREENE, CPA, CFE, MCJ

Craig is a leading fraud examiner and white collar criminologist. With over 30 years of experience, he frequently testifies in cases involving financial fraud, accounting, audit, and other disputes involving financial issues. Craig has led many corporate internal investigations focusing on financial statement fraud, corrupt payments, embezzlement and other occupational fraud schemes. He is an international lecturer on forensic accounting and fraud examination issues. E-mail: craig.greene@mcgoverngreene.com

CONTACT US AT 312.419.1961 OR VISIT www.mcgoverngreene.com
FOR EXPERT FRAUD EXAMINATION AND LITIGATION SERVICES

McGovern & Greene LLP
105 W. Madison Street, Suite 406
Chicago, IL 60602