Fraud Alert

Insights on fraud detection and deterrence

JUNE/JULY 2010

Don't run afoul of whistleblower protections

A fraud contingency plan can guide you through a financial disaster

Shell games
How to know if you're being played

Is your insurer profiting from wrongful denial of claims?

Routine questions can nip fraud in the bud

Wilson & Turner Incorporated

Investigative Consultants

2752 Mt. Moriah Parkway
Memphis, TN 38115

Voice (901) 546-8585
Fax (901) 546-8584

www.wilson-turner.com

Don't run afoul of whistleblower protections

The Sarbanes-Oxley Act (SOX) prohibits retaliation against employees who report suspicions of fraud. Although SOX rules apply primarily to public companies, private companies need to be familiar with the provisions of the whistleblower protection. Otherwise, they could find themselves in violation without even knowing it.

No hassles

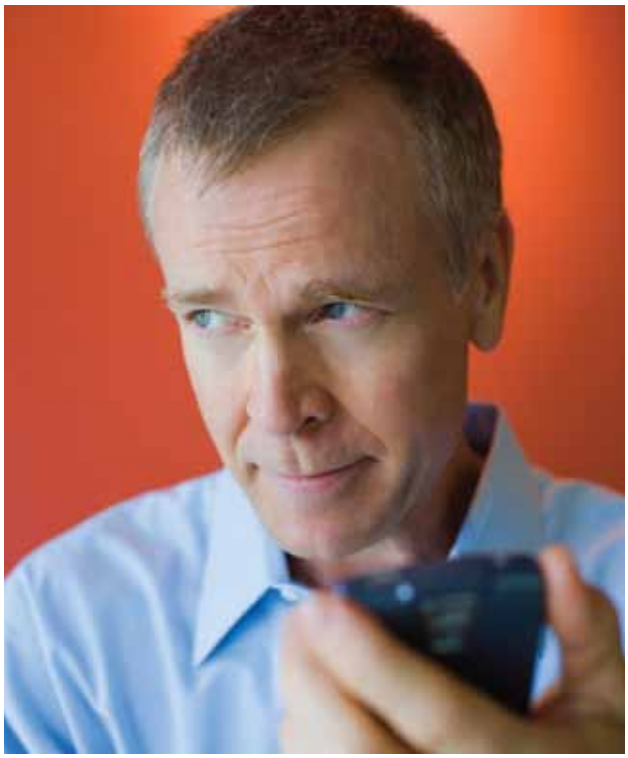
SOX Section 806 prohibits publicly traded companies, including their officers, employees, contractors, subcontractors or agents, from discharging, demoting, suspending, threatening, or discriminating or retaliating against a whistleblower. This includes employees who have filed a complaint or participated in or assisted with a fraud investigation.

But even private companies can be affected by this SOX mandate. In some cases, the Department of Labor (DOL) has held that private businesses have been acting as agents or subcontractors of public companies and are, thus, covered by SOX. Even if you have no dealings with publicly traded companies, today's regulatory climate suggests it's smart to try to abide by the same standards as your public counterparts.

Standard of proof

For employees reporting a retaliatory act, the standard of proof under SOX 806 isn't very high. They aren't required to prove fraud or even that their firing was retaliatory. Employees just need to show that they reasonably believed a fraud was being perpetrated, that they disclosed that belief to their employer or to authorities, and that they were fired within a short time after the disclosure.

If an employee meets the standard of proof, the business must prove by clear and convincing evidence that it would have fired the employee regardless of the whistleblowing. That isn't always



easy to do, and sometimes the DOL may order that the employee be reinstated before there's even a hearing on the merits of the claim.

Avoidance is the best policy

Your best bet is to avoid running afoul of SOX 806 in the first place. Be sure your employees understand how they can report suspicious activity without fear of reprisal by, for example, calling your confidential hotline. (See "Confidential hotlines are critical.") Also make absolutely certain all supervisors understand that retaliation is strictly prohibited.

As part of your fraud-prevention plan, adopt policies that encourage everyone in the company to report suspicious activity. And revise managers' job descriptions to include SOX 806 compliance as one of their responsibilities. At the same time, limit the number of people who receive and document complaints. Keep the sharing of this information on a "need-to-know-only" basis.

Confidential hotlines are critical

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 financial irregularities and thieving co-workers.

Numerous studies have shown that the best way to encourage employee tips is through a confidential, 24-hour hotline operated by a third party. The Sarbanes-Oxley Act requires publicly traded companies to make some kind of anonymous mechanism available, with stiff penalties for noncompliance. But private companies are strongly encouraged to offer one as well.

Providing a hotline isn't enough. Be sure to publicize it to employees, customers and vendors, stressing that you'll protect the identities of all callers and investigate claims until you reach a satisfactory conclusion.

But what if you want to fire an employee who's made a whistleblower report, for reasons unrelated to the complaint? Ensure that you have clear and convincing evidence that your action isn't retaliatory. As a practical matter, that means you need plenty of documentation, including a record of unacceptable performance or activities, with dates, and the action taken following each incident. You may also want to discuss the situation with your attorney before terminating the employee.

Under SOX 806, a whistleblower can sue you individually for wrongful retaliation, and criminal penalties can be as high as 10 years in prison. Even if the whistleblower's accusations are ultimately proven false, your company's image is likely to be tarnished by a prolonged dispute.

Start with an ethical culture

If you aren't aware of all the provisions of SOX 806, become familiar with them now. Even more important, take steps to ensure that your company is held to high ethical standards, which include strong fraud controls, regular audits, and simple and confidential fraud reporting mechanisms. ■

A fraud contingency plan can guide you through a financial disaster

The first thing every Boy Scout learns is to "be prepared." Business owners would do well to remember this motto when they're developing fraud control procedures. Even if you don't believe your employees are capable of defrauding the company, it could happen. But if you have a fraud contingency plan in place, you'll be prepared to handle it.

Keeping a clear head

A fraud contingency plan is your disaster road map. When you learn that a trusted employee has been stealing from you, you'll likely be distressed — which is no time to trust your instincts for damage control. With a well-designed contingency plan, you won't have to rely on knee-jerk reactions.

No contingency plan can cover every fraud possibility, but yours should be as comprehensive as possible. Work with your senior management team and financial advisor to devise as many fraud scenarios as you can dream up. Consider how your internal controls could be breached by an enterprising fraudster, whether a rank-and-file employee, manager, executive or third party. Look at how someone

could defraud the company acting alone or how employees and outsiders might work in collusion.

Next, determine which scenarios would be most likely to occur and which would be most damaging from a financial and public relations standpoint. Then decide what you'll do about them if they happen.

Name names

Your plan should be specific to the risks your company faces and assign distinct responsibilities. Designate one person to lead the overall investigation and coordinate with staff and any third-party investigators. After that, assign specific tasks to knowledgeable managers. Your IT manager, for example, may be tasked with protecting your computer system to prevent loss of electronic records and your head of human resources may be responsible for maintaining employee morale.

Employee communications are particularly important during a fraud investigation. Employees who don't know what's going on will speculate and they may not be particularly circumspect about it. Consult your legal and financial advisors to clarify whether any information should be withheld, but be as honest with your employees as you can.

It's equally important to make your response visible, because it strengthens your fraud-prevention efforts. If employees know you take fraud seriously, they'll be less likely to attempt it themselves and more likely to report suspicious activities on the part of others.

Don't lose your standing

Fraud can wreak havoc with your company's reputation and weaken its standing in the community. Therefore, designate someone to manage external communications. This person should be prepared to deflect criticism and defend the company's stability, as well as control the flow of information to the outside world.

Work with your senior management team and financial advisor to devise as many fraud scenarios as you can dream up.

You'll also need to define the objectives of a fraud investigation. Some companies want only to fire the person responsible, mitigate the damage and keep news of the incident from leaking. Others may want to prosecute offenders as examples to others. Your fraud contingency plan should include information on working with law enforcement in either event.

Change with the times

After you've created and implemented your fraud contingency plan, review it regularly, because employee turnover and new suppliers, customers and products are constants in most companies. Be sure your contingency plan is flexible enough to change with the times. As any Boy Scout will tell you, it's wise to be prepared. ■

Shell games

How to know if you're being played

For a nominal fee, prospective business owners can get a "doing business as" (DBA) certificate from any county clerk's office under the name of their choosing. For many entrepreneurs, DBAs are a cost-effective way to open a small business. And for fraudsters, DBAs can be a cost-effective way to create shell companies they can use to steal from their employers.

Shell companies — businesses with no assets of their own — may serve legitimate business purposes, such as holding another company's assets. But they also may be used to perpetrate fraud.

Stealing on the cheap

Media coverage of shell companies typically focuses on large-scale fraudulent undertakings, including stock market manipulation, terrorist funding, money laundering and tax evasion. The problem has been so great, in fact, that both the Securities and Exchange Commission and the IRS have made changes to tighten regulatory loopholes in recent years to more easily expose individuals who are hiding income.

For most businesses, however, the larger threat of shell companies may be that unscrupulous employees will use them to perpetrate billing fraud. Such schemes can cost a company hundreds of thousands of dollars in losses.

Money for nothing

Billing fraud that uses shell companies can take two forms. In one, dishonest employees set up a shell company to send out — and collect on — fictitious bills. Of course, perpetrators don't even have to send the bills for nonexistent goods and services to the company for which they work. But it's easier, and can help them evade detection, if they do.

Consider, for example, an accounting staffer who knows that her employer rarely scrutinizes invoices for less than $2,500. She can get a DBA certificate for a fictitious business, using a post office box or accomplice's address, and open a business account at a local bank. Voila! She's ready to start billing her employer for services that cost less than $2,500 per invoice.

The second type of shell-company-based billing fraud is a pass-through scheme. Again, an employee sets up a fake company. This time, however, he uses it to buy goods or services his employer requires and then sells them to the employer at a marked-up price. Because the employee's shell company has no overhead or expenses, he pockets the proceeds.

Following the paper trail

Shell company schemes can go undetected for a long time, particularly if the fraudsters are savvy enough to attempt to cover their tracks — and if they don't get too greedy. Most perpetrators, however, leave a paper trail flagged with warning signs that are visible to informed eyes. These include invoices that:

- Poorly define their products or services,
- Have a company address that matches an employee's home address,
- Use a post office box as their return address,
- Have a company name that matches an employee's initials,

- Arrive more than once a month, and
- Show an increased number of purchases over time.

None of these in isolation is proof of fraud, but any of them warrants a closer look. Taking the time to scrutinize a company's operating practices also is wise.

A shell company scam perpetrated by an accounting employee, for example, works only if the employee can pay the invoices or get the shell company authorized as a legitimate vendor. A credit check on a new vendor will reveal whether it has an operating history, and a quick Web search will show whether its name appears outside of your company's records.

System of checks

It's very easy to start a business, but that shouldn't give fraudsters a free hand to rip off or even destroy yours. Familiarize yourself with the signs of shell company abuse and put in place a system so that you'll catch billing fraud before it begins. ■

Is your insurer profiting from wrongful denial of claims?

Your company pays its insurance premiums faithfully, secure in the knowledge you're covered if something goes wrong. Most of the time, you are. Not only is it good business practice for insurers to cover legitimate claims, but it's illegal for them to deny them.

Unfortunately, not all insurers are good, and some may be guilty of bad faith — wrongfully denying insurance claims. This can cost businesses significant aggravation, not to mention legal fees, to combat.

Disagreement or bad faith?

An insurance policy is a contract. The insured agrees to pay premiums and take reasonable steps to prevent injury or damage; the insurer agrees to settle legitimate claims according to the terms of the policy.

Occasionally, you and your insurer might disagree about what is covered or what constitutes a reasonable delay or amount in settlement. But errors in judgment and offers of compromise don't necessarily equal bad faith. Bad faith arises when the insurer sacrifices its insured customers' interests to enhance its own bottom line — and that can involve fraud.

Shady tactics

Outright denial of claims is only one bad faith practice that indicates fraud. Shady operators may also:

- Unreasonably delay investigating claims,
- Attempt to settle claims for less than the amount specified by the policy,
- Bog down the claim process by requiring multiple, duplicative proof of loss forms,
- Fail to settle one portion of a claim to influence acceptance of lesser settlements under another section of the policy, and
- Misrepresent policy provisions related to the claims.

Scammers can illegally deny claims across the country, knowing that fraudulent insurance practices are subject only to state scrutiny and penalties.

After prolonged negotiations, a claim might go to arbitration in an effort to resolve the issues without legal action. At that point, a bad faith insurer might threaten to appeal arbitration awards to pressure the insured to settle for less than the awarded arbitration amount.

Mounting a defense

Defending against such practices can be difficult. There's no federal — only state — regulation of the insurance industry. Thus, scammers can illegally deny claims across the country, knowing that fraudulent insurance practices are subject only to state scrutiny and penalties. These penalties vary, but typically aren't stiff enough to be deterrents and do nothing to compensate claimants that were wrongfully denied.

It's important, therefore, to deal with only reputable insurers. Before you buy, check with industry rating services such as A.M. Best (http://www.ambest.com) or your state's licensing board. If you have a claim, be sure to file it promptly and document all correspondence and communication relating to it.

Insure against fraud

The financial incentives, coupled with inconsistent regulation across states, can make bad faith insurance practices very attractive to dishonest insurers. Basic preventive measures can go a long way toward helping you avoid these types of insurers. But if your insurer seems to be illegally denying your claim you may need to settle the matter in court. ■

Routine questions can nip fraud in the bud

Corporate antifraud programs comprise many parts, including internal controls, fraud prevention training for employees and investigation procedures when fraudulent activity is suspected. But what about spotting and stopping schemes that are still in the larval stages?

Confidential hotlines are a good start. But to head off scams before they come to fruition, some companies periodically call in forensic accountants to conduct employee interviews. Unlike interviews conducted when an actual fraud incident is suspected, routine questioning is used to gather tips about possible misdeeds and gauge the organization's general vulnerability for fraud losses.

Fraud interviewers typically start by establishing some rapport with the interviewee so the employee doesn't feel like the subject of an interrogation. The expert might then ask a series of questions, beginning with very general topics and proceeding to the more specific:

- Do you think fraud is a concern for most companies?
- Is there a fraud problem here?
- If employees or managers were stealing from this company, why do you think they would do it?
- What would you do if you knew another employee was stealing?
- How would you respond if someone asked you to do something unethical?
- Do you know of anyone who might be stealing or taking unfair advantage of the company?

Depending on the responses received, the interviewer may conduct follow-up interviews to support or dispel rumors and accusations. And the expert might advise the company to conduct a thorough investigation of financial records, or to scrutinize a specific employee or the activities of a whole department.

Most routine interviews, of course, don't turn up smoking guns. Conducting them from time to time, however, can highlight internal control weaknesses and uncover employee morale problems that could motivate some to commit fraud. Knowing that management is actively looking for malfeasance will dissuade some potential thieves and promote a more ethical corporate culture.

Know who to trust when fraud occurs

When it comes to fraud impacting a business, the unfortunate reality is that the question is "when", not "if." Wilson & Turner Incorporated specializes in identifying, isolating, and unraveling financial fraud schemes and plotting a path toward financial recovery for the victim organization.

Fraud is present in almost all businesses, with only the internal control and audit processes to keep it in check. When those functions fail, or are circumvented, frauds can quickly grow to devastating proportions.

WTI was established in 1996 to help business, industry, and governmental organizations successfully resolve white collar crime related matters. The firm has particular expertise in resolving employee fraud issues, recovering losses, and protecting corporate assets. WTI provides consulting and expert services to corporations, banks, major law firms, and national and state governments.

WTI specializes in:

- **Fraud solutions**
- **Independent investigations**
- **Employee dishonesty**
- **Due diligence**
- **Commercial litigation**
- **Insurance claims**
- **Computer forensics**
- **Anti-fraud training**
- **Expert witness testimony**

Focused on the investigation and recovery aspects of financial fraud, WTI is experienced in dealing with transition periods, including growth and re-engineering processes; business changes, including takeovers, mergers, and spin-offs; and insurance claims, including professional negligence, Directors & Officers (D&O), Fidelity Bonds, and contractual disputes.

Using sophisticated analysis techniques, WTI conducts forensic and investigative exercises to track fraud losses and identify scheme participants.

Wilson & Turner Incorporated

Investigative Consultants

2752 Mt. Moriah Parkway
Memphis, TN 38115

Voice (901) 546-8585
Fax (901) 546-8584

www.wilson-turner.com