Fraud Alert

Insights on fraud detection and deterrence

YEAR END 2010

Insurance fraud: Spot it and stop it

Bankruptcy scams
When customers don't plan to pay

Using anonymous hotlines to cool fraud

What makes good employees turn bad?

Wilson & Turner Incorporated

Investigative Consultants

2752 Mt. Moriah Parkway
Memphis, TN 38115

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

www.wilson-turner.com

Insurance fraud: Spot it and stop it

Insurance fraud has a timeless appeal among scam artists, but it becomes even more popular when economic times are hard. Slip 'n falls, fake car accidents and even arson are greater threats as people feel a pinch in their pocketbooks.

Unscrupulous individuals sometimes target businesses and their insurance companies as "deep pockets" of wealth. The two largest threats for companies are workers' compensation fraud, in which an employee fraudulently alleges an injury on the job, and property-casualty fraud, in which a claimant alleges personal or property damage resulting from an action by the business. It's critical that you know the signs of such scams and act on any suspicions.

Don't believe every story

Employee insurance scams are most likely to take the form of workers' compensation fraud. Workers may falsify claims, use unnecessary medical services, miss work after an injury has healed or report an off-hours injury as an on-the-job accident.

Although none of the circumstances described below is conclusive in itself without further investigation, prudent employers should be on the lookout for the following common signs of workers' compensation fraud:

An employee reports an on-the-job injury Monday morning, with no witnesses. Workers who get hurt over the weekend pursuing leisure activities sometimes try to turn their injuries into cash by faking an accident at work.

An employee reports an injury just before a seasonal layoff or other work stoppage. A worker who claims an injury just before a strike, layoff or regular shutdown may be looking for a way to collect income during the closing.

A new employee reports an injury. Workers' compensation abusers sometimes have little intention of doing any actual work. Their goal is to get hired and report an injury after very little time on the job.

An employee on recuperative leave is hard to reach. The employee may be "double dipping" — working another job while collecting benefits for an injury that supposedly makes work impossible.

Accounts of the accident differ. The worker may describe the accident differently to the employer than to doctors. Sometimes, accounts by accident witnesses differ from the injured worker's account.

Irregularities mark medical treatment. The injured employee may refuse a diagnostic procedure to confirm an injury, or may change medical providers frequently.

Don't ignore the details

In property-casualty insurance fraud schemes, particular behavior or circumstances may alert businesses that they're being set up. Sometimes the clue lies in the details of the incident underlying the claim and sometimes hints come in the way the report is filed. Red flags include:

Witnesses to a reported accident are unavailable. In variations of this situation, an overly enthusiastic witness or a witness related to the claimant comes forward. Details in the account may suggest that the claimant created the so-called hazard that caused the alleged accident.

The claimant pushes for a quick settlement or accepts a reduced settlement. Sometimes, the claimant threatens the insured with adverse publicity if the claim is not settled quickly.

The claimant is difficult to reach or has a suspicious address. The claimant may use a post office box, an answering service or an unconventional business address to receive communications. Related behavior that may provide a tip-off includes frequent changes in home address and telephone number, a preference for handling business in person, or reluctance to use the U.S. mail.

The claimant can't or won't produce solid identification. Further investigation may show that the claimant has an active claims history under various aliases.

A food poisoning claimant is the only person to become ill. Another suspicious circumstance in claims of illness after eating is the failure to produce any foreign or contaminated substance as supporting evidence.

A food product liability claimant can't produce evidence showing contamination. Typically, the only evidence offered is the package wrapper, can or box.

Don't make it easy

Too often, insurance fraud succeeds because there's no reliable evidence to prove it. To protect against scams, consider installing a security camera system so you can monitor activity on your premises and capture critical evidence of fraud.

And, as with other types of occupational fraud, your employees are your company's first and best defense. If an employee is faking an illness or injury to collect unmerited workers' compensation, his or her co-workers probably will be the first to know. If a fire in your warehouse was set intentionally to hide missing or stolen inventory or to help the department recover from a lackluster quarter, employees who worked there may be suspicious before you are.

Don't forget to collect evidence

Employees can also help you gather and preserve evidence of scams. Be sure to train them to respond properly to potential fraud incidents so you don't lose important information.

If there's an incident on your property, employees should photograph the accident site immediately, and then collect and document specifics such as the:

- Name, address, phone number and date of birth of the injured person,
- Date, time and location of the accident,
- Weather conditions at the accident site (if outdoors),
- Nature of injuries reported by the victim,
- Names, addresses and phone numbers of witnesses,
- Description of the accident and how it happened, and
- Description of the injured person's appearance and attitude.

As well as informing you, employees need to report accidents or emergencies to your company's insurance carrier immediately. They should also relate

Anatomy of a scam

To understand how insurance fraud works, consider the case reported several years ago by Federated Mutual Insurance Company. A pregnant woman stated that she'd slipped on a wet sidewalk outside a business and that the resultant fall caused injuries that ultimately led to a miscarriage.

The woman claimed that the business's owner had failed to maintain the premises properly or warn her of the danger. She provided an emergency room report verifying the miscarriage and demanded a $60,000 settlement. But when the insurance company ordered her medical records directly from the hospital, there was no mention of a miscarriage. She had rewritten the report, and her claim was denied.

any suspicious behaviors or comments that might lead them to believe the incident involves fraud.

Many employees are afraid to "rat out" their fellow workers. So be sure to give them a safe way, such as a confidential hotline, to report their suspicions. (See "Using anonymous hotlines to cool fraud" on page 6.) And include common insurance scams and their warning signs in your company's fraud prevention program.

These simple acts could protect you from some major headaches, and worse — financial losses.

Best defense

Most insurance claims are legitimate, but fraudulent claims built on false or inflated accounts of injury cause significant harm to companies. Staying alert to the signs of potential insurance fraud and training employees to act on their suspicions is the best defense. ■

Bankruptcy scams

When customers don't plan to pay

You've landed a lucrative new account, and the business already has placed several small orders with you, paying in full, on time. The customer is so happy with the products you've supplied that it wants to place a larger order, but has requested that you first expand its credit account.

One of its credit references is a Fortune 500 company, so it seems like a reasonable risk, right? Actually, there's a chance that you're about to become a victim of bankruptcy fraud. Your new customer may be the linchpin in a "bust-out" — one of the more common bankruptcy-related scams. In the current economic climate, many companies are on the brink of banktuptcy — legitimately or otherwise — and you must look closely before extending credit.

Bust out of bust-outs

One of the more popular forms of bankruptcy fraud is the bust-out. Fraudsters create a bogus company — often with a name similar to that of an established, reliable business — to order goods they have no intention of actually paying for. In fact, they plan to sell the products for fast cash, file for bankruptcy and leave you, the supplier, holding the empty bag.

In a variation of the scheme, bogus operators buy an existing company and use its good credit to order the goods. Either way, they sell the products they order below cost, for cash, and then file for bankruptcy, writing off the amounts the suppliers bill.

The owner of a business on the brink of collapse may transfer property to a third party – or, most commonly, a spouse – for little or no compensation.

To avoid becoming a bust-out victim, carefully vet businesses that were formed only recently. Also be wary of established companies with new ownership — particularly if the new owners seem to want to keep their involvement under wraps. Pay particular attention to customers that have:

- Warehouses stuffed with high-volume, low-cost items,
- Disproportionate liabilities to assets,

- No corporate bank account, and
- Principals previously involved with failed companies.

Although none of these conditions is absolute evidence of fraud, any of them may be a reason to proceed with caution.

Disappearing assets act

Bust-outs are far from the only bankruptcy-related scams unscrupulous operators use. In fact, the most common type of bankruptcy fraud is concealing assets, or fraudulent conveyance.

As its name implies, this scheme involves hiding or moving assets in anticipation of a bankruptcy. The owner of a business on the brink of collapse may, for example, transfer property to a third party — or, most commonly, a spouse — for little or no compensation. The third party holds the property until bankruptcy proceedings have concluded, and then transfers it back to the business owner.

Alternatively, the business owner files for bankruptcy and then, with the court's approval, sells property below value to a straw buyer. The owner's relationship with the buyer isn't disclosed, but the buyer holds the property until the owner is ready to reclaim it at an agreed-upon price.

In either case, the goal is the same: to keep property and monetary compensation out of the hands of creditors. If you're one of the creditors the fraudster is attempting to defraud, the Federal Bankruptcy Code allows you to review asset transfers going back as far as 10 years. If you can demonstrate that any of the transfers were done to defraud creditors, you may be able to get them reversed and recover your share.

Stopping stays

Businesses that file for bankruptcy enjoy an automatic stay period, during which creditors may not press them for payment, file lawsuits against them or even call them to ask about future payments. The stay extends throughout the bankruptcy action, with two exceptions:

1. If someone is or has been involved in multiple bankruptcy filings, then the stay lasts only 30 days.

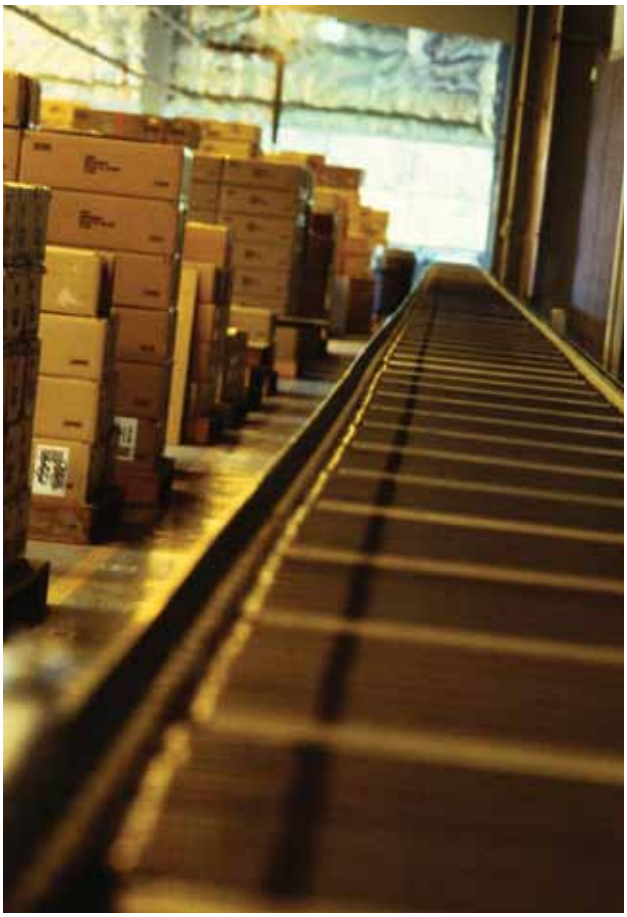
2. Creditors request that the stay be lifted because it's simply prolonging the inevitable — or in the case of fraud, giving the perpetrator more time to dispose of or conceal assets.

A company might, for example, file for bankruptcy the day before the bank is set to foreclose on its property. But a court could lift the stay and allow the foreclosure to proceed, enabling other creditors to resume their actions for payment.

Never say die

Fighting bankruptcy fraud typically requires guidance from financial and legal professionals. The best protection, of course, is prevention, but if you suspect one of your customers is trying to pull a fast one, get help as soon as possible.

When possible, require cash on delivery. If you can't do that, be aggressive about your billing and collection procedures. Legitimate customers will understand your request for payment, and potential scammers may turn to easier pickings. ■



Using anonymous hotlines to cool fraud

The Sarbanes-Oxley Act requires publicly traded companies to have confidential, anonymous reporting systems for employees to report possible misconduct. Even though privately held companies aren't required to implement fraud hotlines, they're doing themselves a disservice if they don't.

According to the Association of Certified Fraud Examiners' (ACFE's) *2010 Report to the Nations*, companies lose more than 5% of their revenue to fraud every year. Organizations with fraud hotlines, however, can cut their losses by more than half — from a median of $245,000 to $100,000. So if your company doesn't make a hotline available to employees, consider what you might be losing.

Compelling evidence

The ACFE has consistently found that employee tips are the best way to uncover occupational fraud. Nonmanagement employees often witness and hear about fraudulent activities, but are reluctant to "tattle" for fear of retribution from co-workers or even supervisors.

Not surprisingly, the existence of fraud hotlines consistently correlates with the number of cases detected by employee tips. According to the ACFE, in organizations that had hotlines, 47% of frauds were detected by employee tips. But in organizations without hotlines, only 34% of cases were detected by tips.

Hotlines have also been shown to reduce the duration of fraud schemes. For companies with hotlines, the average duration of a fraud is 13 months, compared with 20 months for companies that don't offer a hotline.

Avoid voicejail

To be effective, hotlines must be properly set up and operated. If employees aren't assured their reports will remain confidential or anonymous, they're likely to remain silent about what they know or suspect. Similarly, if your tip hotline is open only during business hours, employees won't use it.

Companies that are serious about using their hotline to prevent fraud make it available 24 hours a day. People often decide to report suspicious activities late in the evening or early in the morning. What's more, effective hotlines are staffed by trained professionals, because, when tipsters call, they're likely to be upset or angry and may, therefore, need to be handled with sensitivity. And they're likely to be more honest and open with outsiders who don't personally know the employees involved.

If tipsters are asked to leave a message, many will hang up. Others might report that their supervisor is stealing from the company, but won't leave enough information for you to identify the supervisor, the department or how the theft is occurring. If an interviewer takes the call, he or she can extract the information you need to investigate — without compromising the caller's anonymity.

Extend the line

When you establish a hotline, make it available to customers and vendors as well as employees. These external stakeholders may witness activities or hear rumors that employees choose to ignore or overlook.

Communicate not only that a hotline exists, but also how it should be used: what types of activities

should be reported, and the basic information that must be supplied to initiate an investigation.

Also, establish a plan to ensure the proper people receive any hotline tips. Your human resources department, for example, may receive sexual harassment or discrimination complaints, while allegations of fraud or financial irregularities may be routed to your attorney or outside auditor.

Be visible

It's essential that you publicize your hotline activities. Without revealing identifying details, let employees and other concerned parties know how many calls you've received and, when possible, how they were resolved — for example, whether perpetrators were punished or prosecuted.

People are more likely to use this resource if they believe something will happen as a result. And those contemplating fraud are less likely to proceed if they believe they'll be reported. Hotlines are an important component of your company's larger antifraud culture and help send the message that dishonesty and theft won't be tolerated. ■

What makes good employees turn bad?

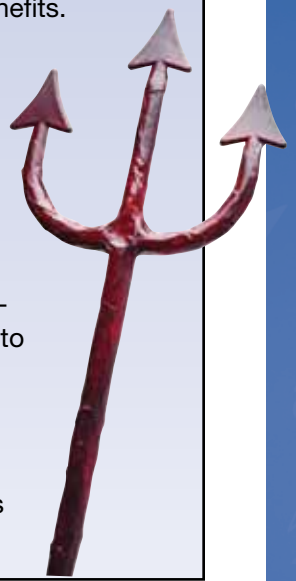
Occupational fraud perpetrators rarely are career criminals. As the Association of Certified Fraud Examiners (ACFE) concluded in its *2010 Report to the Nations*, a whopping 85% of fraudsters in their study had never been charged or convicted of a fraud-related offense.

What makes trusted employees — including those who passed pre-employment background checks with flying colors — steal from their employers? Generally, three conditions are present, a situation fraud experts refer to as the "fraud triangle."

1. Motive. Personal financial pressures such as mortgage troubles, heavy credit card debt, high medical bills, drug or gambling addictions, and divorce can lead employees to commit fraud. In many cases, employees steal out of desperation — they believe they have no other option. However, some perpetrators may simply want to live a more luxurious lifestyle.

2. Rationalization. Otherwise ethical employees may justify theft because they believe they're overworked, underpaid or treated unfairly. These feelings tend to be more common during tough economic times when companies are understaffed and may have to reduce salaries and benefits.

Employees often tell themselves they'll repay the "loan" when their financial condition improves. Or they may rationalize theft by thinking that their company's owners are "rich and can afford it" or that the company owes them more than it's paying. In rare cases, employees are comfortable enough with dishonesty that they don't need to rationalize it internally.



3. Opportunity. Many companies lack sufficient internal controls. But even when there's an internal control system in place, higher-level managers and long-term employees, who are more trusted and familiar with internal control weaknesses, may find ways to override it.

Unfortunately, those in the position to override controls also tend to steal the most. The ACFE reports that frauds committed by owners and executives are more than three times as costly as frauds committed by ordinary managers, and more than nine times as costly as rank-and-file employee thefts.

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