# Fraud Alert

Insights on fraud detection and deterrence

AUGUST/SEPTEMBER 2010



Wilson & Turner Incorporated
Investigative Consultants

2752 Mt. Moriah Parkway
Memphis, TN 38115

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

www.wilson-turner.com

# Getting the goods on inventory theft

When a company suspects that a current or former employee may have stolen inventory, it can be difficult to determine whether the suspicions are true — let alone document and prove the theft. Forensic accountants called in to investigate a suspicion of inventory theft must typically examine extensive records and physical inventory to learn why the shelves are empty. But their job can be made difficult by widespread employee access to inventory, haphazard record keeping and infrequent inventory counts.

## Identifying the problem

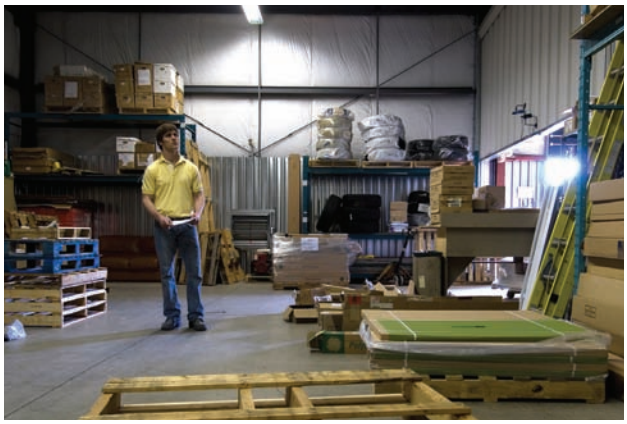
In some cases, a forensic accounting investigation finds that there's been no inventory theft. Items may simply be stored in the wrong place or sloppy paperwork may fail to document their location and current count. So experts review the company's receiving and inspection procedures, for instance, before assuming a theft has taken place. (See the sidebar "Theft vs. oversights.")

However, when experts can find no other plausible explanation for the missing inventory, they look for signs that the company's culture and inventory department are conducive to fraud. For example, a company with poor controls over purchasing, receiving and cash disbursement runs a higher risk of inventory theft. One person performing multiple duties can both commit and conceal fraud.

*In pinning down suspected theft, it's best to do the count in person rather than delegate the job to a possible fraud perpetrator.*

If they believe the inventory could have been stolen, forensic experts comb inventory records for red flags, such as:

- Unusual journal entries posted to inventory,
- Large gross margin decreases,



- Unexpected inventory shortfalls, and
- Unusually large account adjustments after employees perform a physical count.

If one or more of these warning signs are present, the experts set to work verifying the evidence and proving the existence of fraud.

## On the trail

Inventory fraud may leave a paper or electronic trail, so forensic accountants review journal entries for unusual patterns. For example, an entry recording a physical count adjustment made during a period when no count was taken warrants suspicion. The experts follow up by tracing all unusual entries to supporting documents.

Financial records aren't the only evidence. Vendor lists may show suspicious patterns, such as post office box addresses substituting for street addresses, vendors with several addresses, and names closely resembling those of known vendors.

Even if they've found no sign of nonexistent vendors, forensic experts look at all vendor invoices and purchase orders for anomalies. For example, an unusually large invoice or alleged purchase that doesn't involve delivery of goods warrants a closer look.

Discrepancies between the amounts due per invoice, the purchase order, and the amount actually paid also merit investigation. Experts further familiarize

themselves with the cost, timing and purpose of routine purchases and flag any that deviate from the norm.

### Taking a count

It's important to confirm the company's physical inventory as well. Although a count may disrupt normal business routines, it's an effective way to learn exactly what merchandise is missing. If done properly, it also may lead directly to the thief.

Forensic experts sometimes recommend hiring an outside inventory firm to not only perform the count but also value the inventory. Generally, a hired inventory team is scheduled to arrive quietly and unexpectedly so that it might catch the perpetrator in the act. Warehouse activity must be watched carefully once employees realize a count is imminent. Thieves may make hurried attempts to shift inventory from another location to substitute for missing items they know will be discovered.

Inventory at remote locations also can disappear, so forensic experts often will confirm quantities with the storage facility or go with company officials to personally inspect them. In pinning down suspected theft, it's best to do the count in person rather than delegate the job to a possible fraud perpetrator.

### Theft vs. oversights

Before assuming theft, forensic accountants check to see whether the items were really stolen, because the issue may simply be one of poor record keeping. Items might be on the premises, but in a different location, or they might have been shipped to customers or never delivered by vendors. A company without a location assignment for each item, an effective method of keeping tabs on overflow stock and a well-run returns system can easily misplace inventory.

Employees fail to notice short vendor shipments because of lax receiving and inspection procedures, and unobserved vendor overcharges can also give the appearance that inventory has been stolen. Forensic accountants look for trouble in these areas if the company lacks proper transaction, approval, authorization and documentation procedures.

Finally, some companies fail to bill customers for shipments because the shipping and billing functions don't work in tandem. Obviously, this can cause inventory to disappear without explanation and must be fixed immediately.

### Proving the theft

Even at companies where inventory policies and procedures are lax, it's possible to build solid evidence of theft. But it requires an experienced fraud expert and the full cooperation of a company's management. ■

# Flight of the phoenixes

## Vigilance can help ground fraudulent companies

When a company goes bankrupt, honest owners or directors do everything they can to hold creditors' losses to a minimum. When it becomes clear the business can't be saved, they halt trading (in the case of public companies), hire professional advisors to help guide them through bankruptcy proceedings and generally arrange for orderly liquidation.

Less scrupulous people use somewhat different tactics. They may, for example, deliberately sell off assets so there isn't enough left of the company to justify creditors bringing in turnaround or bankruptcy experts. Worse, they may attempt to profit from bankruptcy. Knowing how to spot these "phoenix" companies can help prevent you from getting burned.

## A rose is a rose

Owners of a bankrupt company might sell the assets to themselves as owners of a new company that is in the same or related business. The new company may even have the same or a similar name. There's nothing wrong with such companies if some or all of the directors or owners buy the assets at fair market value and use them to attempt to build a financially strong successor company.

There is something wrong, however, if the principals intentionally ran the old company into the ground to avoid liabilities, or if they transferred assets to the new, phoenix company at below-market value shortly before or immediately after the demise of the original business. Those are just some of the signs that fraud is afoot.

According to the International Association of Insolvency Regulators (IAIR), phoenix companies are becoming less common as tighter regulations force more accurate financial reporting among both public and private companies. However, because there are legitimate reasons for solvent businesses to establish subsidiaries or parallel operations, it can be difficult to detect phoenix activity until the transfer of assets, customers and goodwill has been completed.

## Smelling a rat

Signs of trouble may be apparent to those who look carefully. Phoenix companies often are formed with minimal share capital, for example. Also be wary when:

- A company opens its doors either immediately before or within a year after the failed company has publicly stated its imminent demise,
- Some or all of the directors and other senior executives and many employees of the debtor business now work for the new company,
- A number of preferential payments are made to creditors of the insolvent company before it goes out of business so that those creditors will be more willing to supply the new company, and
- Substantial liabilities are left in the insolvent company when the new business is formed.

Before agreeing to do business with these new companies, potential customers and suppliers should

check business references, scrutinize directors' and owners' backgrounds, and learn why the original business failed.

## Catching the perpetrators

While there are civil and criminal remedies for creditors to pursue against phoenix companies, unsecured creditors of the bankrupt business are most likely to suffer. Creditors are most likely to spot potential phoenix activity early, but they may not take action after operators of the phoenix business pay outstanding bills in an effort to keep supply lines open.

There are no definitive statistics on the incidence of phoenix companies, in part because bankruptcy fraud often is perpetrated in conjunction with other types of fraud. Because fraud investigations can be complex and time-intensive, bankruptcy fraud may not be included in indictments if evidence of tax fraud or embezzlement is sufficient for criminal convictions.

The IAIR says, however, that phoenix companies are most common in the construction, transportation, hospitality, and clothing and textile industries. Of course, that doesn't mean phoenix companies don't crop up in other industries. No sector is immune to fraud.

## Controls work

The good news about phoenix companies is that they can be contained. The better news is that more stringent government regulations and heightened financial scrutiny of companies and the people who run them is making it easier to do so. ■

# Mistake or misstep?

## How to survive an IRS audit

Given the complicated nature of U.S. tax laws, it's almost inevitable that mistakes creep into business tax returns. The IRS understands that. The IRS even expects it, to some extent, and is willing to work with companies to resolve errors. The challenge is to convince the IRS that errors are, indeed, errors and not attempts to cheat on your taxes.

*If tax fraud comes up during the audit, stop talking. Ask for a recess to confer with your tax advisor and call legal counsel, if necessary.*

Sarbanes-Oxley (SOX) has only increased that challenge for public companies. And although privately owned companies aren't bound by SOX regulations, they're also susceptible to intensified IRS scrutiny. IRS examiners are looking for fraud, and you need to be able to prove that any mistake they find is an honest one.

### Avoid triggers

Of course, the easiest way to survive an audit is to avoid making the mistakes that will trigger one. One area of particular interest to tax authorities is executive compensation. Auditors include executives' personal tax returns in their corporate audits, hoping to find discrepancies that will point to abuses. This practice's greatest impact is on big business, but even smaller companies must ensure they're complying with tax laws governing use of company credit cards, spousal travel and other executive perks.

Avoiding less obvious errors should be of more immediate concern. Understating or overstating income, miscalculating deductions, taking improper tax credits and incorrectly reporting employee compensation are among the inadvertent sins that can trigger an IRS audit.

### Preparing for the audit

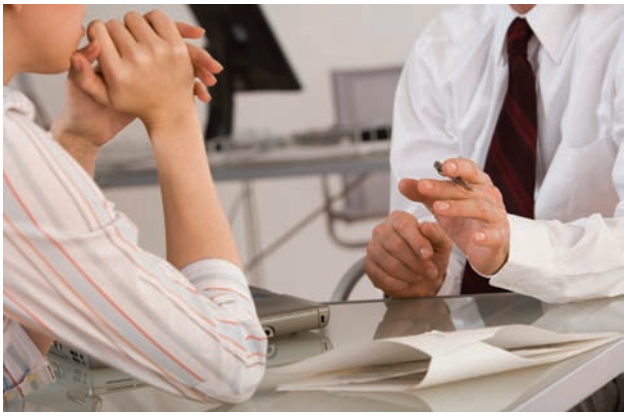
As soon as you learn your company is going to be audited, get in touch with your tax advisor. You'll need expert assistance to avoid unnecessary complications. Then, to give yourself time to prepare, request that the IRS postpone the audit. You'll want to review your records carefully and reconstruct any missing documents. Organize all the records the auditor may need to review to demonstrate that your organization is conscientious and cooperating fully.

If possible, avoid hosting the audit at your business. Instead, arrange to meet at the IRS's or your tax advisor's office. That helps keep the focus on the issues, rather than on your company's operations.

### Be brief and cautious

Once you're in the audit, be brief. Provide all the information the auditor requests or that is required to support your case, but don't volunteer anything more. At the same time, don't hesitate to defend your position regarding any disallowances the auditor may be considering.

One word of caution, however: It's fine for you to negotiate, but negotiate only the issues, not the amounts. Telling an auditor you can't pay the bill won't make any difference in what you owe.



Finally, if tax fraud comes up during the audit, stop talking. Ask for a recess to confer with your tax advisor and call legal counsel, if necessary, and let those professionals take it from there. You also may ask to speak to the auditor's manager if you feel you're being treated unfairly. But don't try to handle a fraud allegation yourself.

### Walk the line

You probably can't expect to come out of an audit scot-free. Even if the auditor agrees you weren't attempting to defraud the government, you'll likely owe additional taxes and a 5% penalty on any amount you've underpaid. But that's better than the 75% penalty assessed on taxes that weren't paid due to fraud. So make sure you use an audit to convince the IRS you haven't crossed any lines. ■

# Don't let botnets turn your computers into zombies

Are you harboring a criminal? You could be, if you're a "zombie" linked to a botnet. No, that isn't sci-fi speak for an alien tied to the mother ship. Zombies are computers infected with spyware and linked in sophisticated, software robot networks called botnets.

According to a June 2010 article in the *Atlantic Monthly*, approximately 25% of the billion computers in use around the world are linked to a botnet. Most users don't know their computers are infected, but some of these insidious programs can cause major damage, including emptying online financial accounts.

### Remote control

Here's how botnets work: Hackers — often based in Eastern Europe — create malicious programs they distribute through e-mail attachments and downloads. Once the program is installed on a computer, the originator can control it through an Internet Relay Chat (IRC) system and scan for specific information.

In most cases, criminals then use the purloined host computer to send spam e-mails that spread viruses or gather data such as passwords and financial information. MessageLabs, a computer security firm, has estimated that more than 80% of all spam originates from botnets. A single Internet service provider is capable of generating more than a billion spam e-mails in a 24-hour period.

### Breaking up business

Botnets can target critical operations, with serious consequences. Just this summer, international authorities nabbed the computer hacker alleged to be behind the Mariposa botnet. Mariposa is credited with infecting more than half of Fortune 1,000 companies and dozens of major banks since it first appeared in 2008. Other botnets have been known to infiltrate hospitals, jails and government agencies, including the Defense Information Systems Agency.

One of the more serious dangers for companies are botnets that launch "denial of service" attacks. The criminals operating such botnets order the computers in their networks to flood a business's Web site with traffic, overloading it. Unless victims are willing to fork over protection money, denial of service attacks can cost them many thousands of dollars in lost revenue.

### Maintain security

Security software can help you fend off botnets. Make sure your network and all individual computers have up-to-date protection and warn employees against turning security software off, even briefly.

Unfortunately, your company may experience a botnet attack despite taking every precaution. "Black hat" programmers are continually refining their software to avoid detection and stay one step ahead of the security firms. If you see signs of infestation, don't hesitate to contact a computer forensics expert. ■

## Your company's write-offs may be erasing theft

Skimming, or removing cash before it has been recorded in a company's books, is one of the most prevalent forms of occupational fraud. Some of these schemes are easy to spot, but skimming via write-offs isn't one of them.

### Lifting the fog

In this type of fraud, a crooked employee writes off an account as uncollectible and then keeps cashing the unsuspecting customer's checks. The account is no longer active, so nobody but the fraud perpetrator expects payments. The books are balanced, but the company doesn't have the money the books claim, and the customer isn't being credited for payments made.

If you've recently noticed a larger number or dollar value of write-offs, as well as customer complaints about their accounts, skimming may be to blame. Gaps in the sequence of invoices could indicate a thief is invoicing a customer for payments and then embezzling them. Duplicate credit memo numbers can mean someone is processing credit memos twice.

### What experts look for

When forensic experts investigate possible write-off fraud, they go over the company's books and records for documentary evidence, and also check for lax supervision of employees with access to receivables records. If a company doesn't require write-off exception reports or its owners or executives don't personally approve all proposed write-offs, dishonest employees have the freedom they need to write off good debts.

Companies also make it easier for employees to commit this scam if they fail to rotate assignments among staff members and allow just one person to process a single transaction from beginning to end. Forensic accountants check to see which employees open mail, log transactions and reconcile daily cash receipts and bank statements. If the same person is performing all these functions and fraud is suspected, that employee could be the suspect.

Likewise, accounting staffers who refuse to take vacations may be afraid the checks they're skimming will arrive during their absence. Some guilty employees will even refuse promotions that would interfere with their (more lucrative) frauds.

### Out in the open

If you suspect someone in your organization is perpetrating a write-off scheme, talk to a fraud expert. The signs can be subtle, but if they're there, forensic accountants will drag them — and the thief — out into the open.

# 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**