Fraud Alert

Insights on fraud detection and deterrence

FEBRUARY/MARCH 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

Fraud damages

Get the award you deserve

When a business or individual has been the victim of fraud, it's only fair that the perpetrator be required to repay what was stolen. Courts may — and in some states must — order restitution, but judges don't always know how much a company has actually lost. Working with victims' attorneys, forensic accountants can calculate damages in accordance with state laws and help prepare presentations that convince judges to accept the results.

Harder than it seems

At first glance, calculating restitution may seem like an easy process: Someone steals $10,000, so he or she should repay that amount, perhaps with interest. But what about the profits the business lost because of the fraud?

The answer to this question varies from state to state, and even from case to case, but accountants typically use either the "benefit of the bargain" or "out of pocket" rule to determine damages. The appropriate method depends to some degree on the location and nature of the fraud. But in most cases, the benefit-of-the-bargain method results in greater restitution for victims.

Take, for example, a hypothetical feed company that decides to buy and race a Thoroughbred horse for promotional purposes. A horse dealer locates a suitable animal valued at $1 million, but offered at $900,000 because the current owner is retiring. In truth, however, the owner is selling the horse because it hasn't lived up to expectations and is actually worth only about $750,000 — information the dealer has known for several weeks. Putting aside the buyer's failure to perform proper due diligence, how much should it be able to expect in restitution?

Under the out-of-pocket rule, the company would be awarded $150,000 in damages, or the difference between the horse's real value and the amount paid for it. Using the benefit-of-the-bargain rule, however, damages would be calculated at $250,000 — the difference between the dealer's misrepresented value and the animal's true worth.

Profitable approaches

Clearly, victims prefer the benefit-of-the-bargain method, which allows them to recover not only their actual losses and fraud-related expenses, but also lost profits. The appropriate method for calculating damages will vary according to the specifics of each case. But accountants may use several approaches to calculate lost profits when the benefit-of-the-bargain rule applies. They include the:

Benchmark, or yardstick, approach. By comparing the fraud victim's corporate profits to those of another, similar company that wasn't defrauded, experts can determine reasonable damages. This method is particularly appropriate for new businesses or franchises.

Hypothetical, or model, approach. Also typically appropriate for new businesses with little history, this method requires accountants to first gather marketing evidence that demonstrates potential lost sales. After calculating the total, experts subtract the costs that would have been associated with the lost sales to arrive at lost profits.

Pursuing civil remedies

Establishing damages for restitution is one thing. Collecting them may be another.

In many criminal cases, perpetrators aren't required to begin paying restitution until they're released from prison. In addition, victims who aren't named in the indictments handed up against the fraudster aren't eligible to receive restitution. And, in many cases, the perpetrator already has spent or hidden the proceeds of the fraud.

Many victims, therefore, seek civil judgments as well as criminal convictions against fraud perpetrators. Civil actions can force crooks to sell or forfeit assets to help pay restitution. Also, while criminal orders affect only property of the defendant, civil forfeitures can include assets taken by the perpetrator's family members or friends.

Another advantage of civil actions is that criminals rarely want to link themselves to the spoils of their crimes, so defendants often don't contest them. In such cases, victims are spared the cost and effort of going to trial. Instead, the cases are handled administratively. Filing a civil action has no effect on criminal proceedings, and victims may receive restitution orders from either or both.

Before-and-after approach. For longer-established businesses, accountants look at the company's profits before and after the fraud compared to profits during the time the fraud was being committed. The difference is the lost profits.

Each method may be appropriate in certain circumstances, but accountants must work with attorneys to determine which is best for the particular case. Net income rarely is the basis for assessing lost profits, however. Lost-profit awards are taxable, which means they're calculated on a pretax basis, making net income invalid for computational purposes.

Road to recovery

Regardless of the damages calculation method used, fraud victims and their attorneys can rely on accountants to assess actual financial losses as a result of fraud. Courts must know how much damage has been done before they can consider restitution, and victims have little hope of recovering their losses without an expert's estimate. ■

Trust, but verify

How to guard against bookkeeping fraud

The bookkeeper is one of any company's most trusted employees. Unfortunately, that trust isn't always prudent. Accounting department employees are ideally positioned to embezzle from their employers, and, in the face of expensive habits, mounting debt or other financial pressures, some of them give in to the temptation for fraud.

Less means more

When bookkeepers go bad, there are plenty of ways for them to steal without alerting owners or managers to irregularities. One simple method is to include a "less cash" amount when depositing checks to the company account — an amount that goes directly into the bookkeeper's wallet. Another tactic is to open a sham account in the company's

name with his or her name as signatory, and then deposit payments to the business in that account.

Outright forgery is possible, as well. Employees may forge an authorized signature on checks payable to themselves, or send fraudulent "letters of authority" to the company's bank. The letters give the bookkeeper unauthorized access to certain accounts.

Stop it before it starts

One of the best ways to guard against bookkeeper fraud is to segregate duties as much as possible. Don't let one employee authorize, sign, post and reconcile checks while also handling every deposit. If you don't have the staff needed to adequately segregate duties, request that bank statements be mailed to your home. Then review them for anything unusual before you pass them to your bookkeeper.

You also may want to work with your bank to prevent "less cash" deposits or unauthorized new accounts, and to require verification of any "letter of authority" or other document that opens financial doors. And talk to an outside financial expert about regularly reviewing your company's financial records.

Signs of trouble

Above all, recognize that, given the right set of circumstances, anyone could be willing to commit fraud. Even the staff member you've rightfully trusted for years may come under enough personal financial pressure to be tempted to steal.

Closely scrutinize your bookkeeper if he or she:

- Frequently takes work home or works late in the evening or on weekends,
- Is reluctant to take vacation time,
- Becomes defensive or resentful when questioned about records,
- Fails to keep deposit records, supplier correspondence and other important documents properly organized,
- Explains away tax delinquency notices as government errors,
- Insists on handling activities such as picking up mail or liaising with financial contacts, or
- Suggests that you get rid of your outside accounting firm to save money.

None of the above is proof of fraud. There may be reasonable explanations for these and other potentially suspicious activities. But if they occur, don't ignore them. You may simply need to add more controls to your financial operations. If you're really suspicious, though, consider bringing in a forensic accountant to investigate.

Employees may forge an authorized signature on checks payable to themselves, or send fraudulent "letters of authority" to the company's bank.

Abuse of trust?

Bookkeepers occupy positions of trust in any company. If an accounting staffer no longer deserves your trust, it's better to know as soon as possible — before this employee has time to cause serious and lasting damage. ■

Your computers might be at risk … from your employees

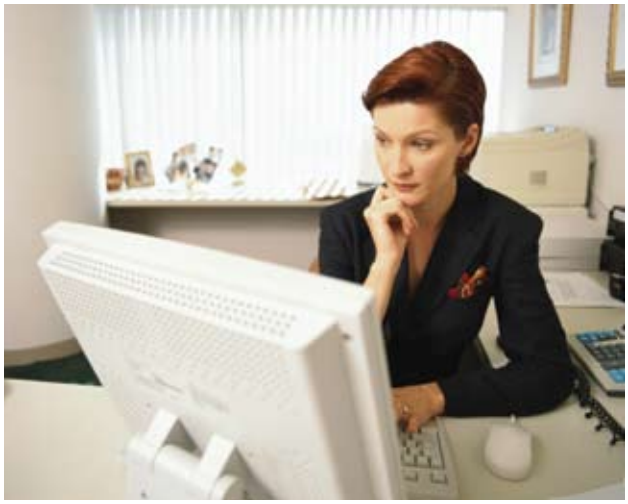
You use firewalls and encryption to protect your business's computer system from outside predators, but do you guard against the fox that's already in the henhouse? Employee computer crime is a real threat, and you must consider its possibility in your fraud-prevention program.

No skills required

Internal computer fraud can include any of a number of transgressions, from illegally copying software to stealing trade secrets to outright theft of company equipment. It can occur at any point in the system: data input, software, data storage or data output.

The input stage, however, typically offers the easiest means for theft. Someone stealing inventory, for example, can update the system to indicate the inventory has been scrapped. The action requires no particular computer skills; the perpetrator just needs to know how your system works. It may be a little harder to damage or change stored data files, but a determined employee with some advanced knowledge of your system can do it. And anyone with access can copy or print output.

Virtually every employee is probably using your system for personal reasons, whether to pay bills, shop for birthday presents or send personal e-mails. Unless such activities are consuming an inordinate amount of time, you probably regard them as benign.



Most of the time that's true, but there are exceptions: If an employee is sending sexually harassing e-mails through the company system, for example, you may be legally liable.

Be a culture vulture

Employees must use your system to keep your business going. And to do that effectively, they must know how the system works. The challenge, therefore, is to give your employees all the knowledge they need to perform their jobs and, at the same time, prevent them from using it against you.

One way to do this is to create a business culture that's hostile to fraud by:

- Identifying areas of greatest risk,
- Creating ethics policies,
- Stressing integrity at all levels of the organization, and
- Ensuring that all employees are effectively supervised.

In addition, when you train your employees in computer usage, instruct them in security and fraud prevention as well.

Take control

More practically, develop a strong internal control system for your IT network. At its most basic, this means segregating duties and restricting access to system resources. But you also must monitor servers, back-ups, e-mails and Internet activities. Employees may experience a small loss of privacy, but you own your company's computers and networks, and you have the right to protect them. Just let employees know up front that you'll be randomly monitoring their computer activities and that you regard monitoring as a routine part of doing business.

Perhaps the most important strategy to protect against internal computer fraud, though, is to know

who has access to what data and how that access is controlled. If you have your own server, keep it in a locked room and log everyone who enters and exits.

Require employees to have passwords for their computers and for particularly sensitive files stored on them. To be effective against intruders, passwords should be complicated. They should include numbers and upper- and lowercase letters, and they should be changed frequently. Also be sure to warn employees against writing them down and leaving them in a readily accessible location — such as taped to their monitors.

Lock the back door

Keep in mind, too, that disgruntled or recently fired employees can use purloined passwords to gain remote access to your company's network. Once in, they can do untold damage by adding, deleting or altering files.

If you must let someone go, be sure to disable his or her access authorizations immediately, and require everyone in his or her department to change passwords. You might also ask your systems administrators to check the files and systems to which the departing employee had access. Employees who sensed their firing was imminent have been known to install programs that will later delete files.

Recognize a real threat

Obviously, you need to protect your computer systems from external security threats, but it's important to recognize that the greatest threat may come from within. Even your most trusted long-term employee is a bigger risk than an anonymous hacker. ■

The unkindness of strangers: Charity scams

The past decade has seen its share of devastating natural and man-made disasters — and corporate citizens have generously donated millions of dollars to help the victims. Unfortunately, scam artists have been only too eager to take advantage of such donor largesse. Fraud perpetrators, pretending to represent disaster aid charities, crawled out of the woodwork only hours after January's Haiti earthquake. And the recent economic crisis has been a boon to those who falsely claim they assist the hungry and homeless.

Before you give money to a group — whether it purports to represent an international disaster relief fund, a national veterans charity or a community food bank — investigate and verify it is what it claims to be. A number of Web sites, including the Better Business Bureau (www.bbb.org), the IRS (http://www.irs.gov/app/pub-78) and GuideStar (www2.guidestar.org), can help you separate the real nonprofits from the imposters. State attorneys general monitor charities as well.

Common sense can also help prevent your company and employees from falling for charity scams. For example, you should never:

- ✧ Send cash donations — and always make checks payable to the charity rather than to an individual,
- ✧ Be fooled by impressive-sounding names or those that resemble names of reputable organizations,
- ✧ Feel pressured — legitimate charities should welcome your gift whenever you send it,
- ✧ Click on a charity link that arrives via an unsolicited e-mail, or
- ✧ Give to an organization you're unable to fully investigate through a government office or agency, or charity watchdog group.

Surrounded by so much need, companies understandably want to help. By following a few simple steps, you can help ensure you and your employees don't become victims yourselves.

Alter ego companies tempt troubled business owners

For some business owners, bankruptcy is simply not an option — even when it's the only option. Faced with impending financial collapse, they instead set up alter ego companies that allow them to divert assets while hiding income and ownership from existing creditors. But it can be difficult to prove that one company is really just a disguise for another.

Shams vs. legitimate companies

Alter ego companies are essentially sham subsidiaries set up by parent corporations with something to hide. Owners divert assets such as inventory and accounts receivable payments from the failing company into the alter ego company — and their own pockets — before the original company is forced out of business. The first company may have virtually no financial worth, but the assets of the alter ego company are protected from bankruptcy proceedings by virtue of its seemingly separate operating status.

One problem in identifying fraudulent subsidiaries is that it's perfectly legal for corporations to limit risk by setting up separate, subordinate firms. Even if they're wholly owned, these companies function independently in terms of sales, billings, assets and management. Legitimate reasons for such companies include tax and profit-sharing advantages as well as liability limitations.

Legitimate subsidiaries, however, won't use their parent companies' letterhead or telephone numbers. Often, they won't share officers, directors or employees or work with the same attorneys and accountants. And the parent company won't pay most of the subsidiary's expenses. In many cases, the parent and subsidiary aren't even involved in the same business.

Asking the right questions

Of course, fraudulent companies aren't always easy to spot. They generally require financial experts to expose them and multiple pieces of evidence to support any legal action against them.

Key questions experts might ask include:

- Has there been a substantial reduction in sales at the original company? If so, have customers actually stopped buying or are they just being billed by the alter ego company?
- Have all accounts receivable payments been properly deposited in the original company's account?
- Are the two companies' product lines identical?
- Does the original company dictate policies and procedures for the subsidiary?

Investigators also consider the number of "related-party" transactions between the companies. Related parties are those that either control or are controlled by a company, as well as officers, directors and their families. In transactions involving an alter ego company, there may be special terms or conditions that help the original company redirect funds to the subsidiary.

Signs are subtle, not invisible

Alter ego companies, as opposed to legitimate subsidiaries, typically have one purpose: to help their owners perpetrate fraud. The signs may be subtle, but forensic accountants and other experts can expose these schemes and help creditors and others recover what's owed them. ■

This publication is distributed with the understanding that the author, publisher and distributor are not rendering legal, accounting or other professional advice or opinions on specific facts or matters, and, accordingly, assume no liability whatsoever in connection with its use. In addition, any discounts are used for illustrative purposes and do not purport to be specific recommendations. ©2010 FAfm10

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