



# fraud alert

october/november 2006

## **Need an expert?**

**Add a CPA to your  
fraud litigation team**

## **Fear factor**

**Risk of detection dampens  
employees' ardor for fraud**

**How computer forensics  
experts snare evidence**

## **Don't get pinched**

**Watch expense accounts for signs of cheating**

## **Fraud to watch for:**

**Domain name registration scams**



**McGOVERN & GREENE** LLP

Certified Public Accountants & Consultants

105 W. Madison Street, Suite 406  
Chicago, Illinois 60602

# Need an expert?

## Add a CPA to your fraud litigation team

Even the most extensive and effective fraud prevention program can't guarantee your company will escape fraud-related legal action forever. If you decide to initiate a civil suit or press criminal charges against an employee, you'll need every resource at your disposal. And one of the most critical is the expertise of a certified public accountant.

### Expert in your corner

Fraud cases can involve anything from falsified financial statements to employee embezzlement, tax fraud or insurance scams. But typically they have one thing in common: They involve large amounts of complex financial documents. Experienced CPAs can help your legal team collect and summarize such documents, and they may be able to reconstruct lost or stolen records.



Because CPAs understand internal controls, accounting systems and financial reports, they can help uncover the full extent of any fraud. They also can be enlisted to analyze and translate financial data for attorneys, insurers and other interested parties.

As a case moves forward, a CPA can be equally valuable with depositions, helping to frame questions that attorneys will ask witnesses. They also are skilled at spotting inconsistencies and flaws in witness testimony and evaluating the opposing side's evidence for weaknesses or inaccuracies.

### Go to court with confidence

Once a case gets to court, a CPA can serve as an expert witness to help shore up your position with

a judge or jury. CPAs with trial experience know that courts aren't interested in dry recitations of facts and figures. A good expert witness, therefore, puts the numbers in a framework that the judge and jury can understand. That framework is carefully constructed to demonstrate that the expert's conclusions are logical extensions of the facts.

While those and other services will be useful in any legal proceeding, a CPA uses different skills to bear on different types of cases. In civil actions, for example, plaintiffs must prove they suffered damages and then determine the extent to which the monetary loss from those damages was attributable to the defendant.

If your company is the plaintiff in a civil suit, a CPA can create a damage model based on factors such as your executive compensation compared with that of other companies, investment rates of return, conditions that affect your business results (including cyclical or seasonal fluctuations) or other considerations appropriate to the business situation and case. Using that model, the CPA will determine monetary damages to your company. A CPA also will review an opposing expert's damage report, and, depending on which state or federal jurisdiction is involved, may help determine the amount of interest that can be added to damage awards.

If you're the defendant in a civil suit, a CPA can review the plaintiff's damage model and prepare an alternative estimate that supports your case. A CPA could, for example, use different tools to value your business and arrive at a lower assessment of the financial damage caused by fraud.

### Other assistance

In criminal cases, CPAs can dig through complicated financial transactions to find evidence of deliberately disguised criminal activity, or determine exactly how a fraud was committed. If someone has been stealing inventory, for example, or improperly billing for products, a CPA can review financial records not only to pinpoint the methods used, but also to quantify the amount that was stolen.

It's unwise for companies to wait until legal action looms before reviewing their compliance and internal control procedures. But when this is the case, while examining your records to prepare for court, your

## Understanding CPA qualifications

Talking to a qualified CPA can be an important first step in building a solid fraud litigation case. But it's also important to match the CPA's qualifications to the type of fraud. Fraud encompasses a multitude of sins, and individual CPAs aren't experts in all of them.

Courts are becoming more selective about the expert testimony they will admit, so you should look at potential CPA consultants' credentials and methodologies to select the best one for your trial team.

All CPAs have college degrees and have passed national examinations. In addition, they are required to obtain professional continuing education credits to remain licensed. Some CPAs, however, are certified fraud examiners, having earned a CFE designation from the Association of Certified Fraud Examiners. Others have business valuation credentials from the American Institute of Certified Public Accountants or the National Association of Certified Valuation Analysts. Still others earn graduate certificates in forensic accounting or other postgraduate certifications.

CPA can identify best practices to help you avoid such situations in the future.

A CPA also may be able to help you stay out of court entirely if you and the opposing party agree that mediation or arbitration are preferable to long, costly litigation. In such cases, a CPA can act as an


objective negotiator, helping you reach a financial settlement that both parties consider fair and acceptable.

## Working with a CPA

When engaging a CPA to work on a fraud case, understand that most communication between these experts and their clients is not privileged. Thus, you may not want to hire a CPA yourself. Instead, have your outside attorney — rather than in-house counsel — retain the individual so all attorney/client communication will be privileged.

CPAs may be consultants on your case, or they may serve as expert witnesses. If you're hiring an expert witness, you'll need to remember that you're not hiring an advocate. Instead, you're hiring a specialist who will remain objective in assessing facts and preparing positions.

## Simplifying matters

In any case involving fraud — whether it goes to court or to dispute resolution — CPAs are familiar with the latest financial and economic concerns and requirements. When you need them most, they can analyze and explain complex concepts and facts in simple terms so you, your attorneys, judges and juries will have all the information needed to decide the case. As such, a CPA is an indispensable member of your litigation team. 

# Fear factor

## Risk of detection dampens employees' ardor for fraud

Do your employees feel like they're being watched? If they don't, they may be emboldened to steal.

As most fraud investigators know, the fear of getting caught is one of the most powerful deterrents. In the same way that putting more police officers on the street tends to reduce crime, making your antifraud activities more visible can discourage fraudsters.

Historically, businesses have relied on internal controls to defend against fraud. But as many companies have learned the hard way, employees bent on fraud can find their way around internal controls if the incentive

outweighs the risk. Businesses must, therefore, be sure their employees — including senior executives — see the risks of committing fraud as being greater than the rewards.

## Perception of detection

There are a number of ways to increase the perception of detection among employees, but the first is education. An ongoing, visible fraud education program fosters the belief that anyone who commits fraud will be caught, simply by demonstrating that fraud is always on the company radar screen.

Fraud education should begin with employee orientation and continue with ongoing employee training programs. Familiarize employees with your company values and expectations, and train them to know what constitutes fraud. Educated employees aren't only more likely to notice and report fraud if they spot it, but they're also less likely to be tempted to perpetrate it.

Setting up a confidential tip hotline also can help create an environment of vigilance, particularly if you routinely publicize nonspecific statistics about the calls it generates. If, for example, the employee newsletter prints statistics regarding the number of calls received and the actions taken as a result, employees may be more likely to view the hotline as a viable, nonthreatening means of reporting suspicious activities. And, again, you'll communicate that the company takes fraud detection and prevention seriously.

### Take it to the top

While education and hotlines can help drive thoughts of fraud out of the minds of line employees and middle managers, the biggest schemes often stem from people higher in the chain of command. As high-profile corporate scandals have shown, CEOs and CFOs aren't immune to the temptation to defraud their companies and their shareholders.

One way to suppress such temptations is to ask senior managers whether they are aware of any fraud in the organization. CEOs who commit fraud often must enlist an accomplice or two. When financial advisors or auditors ask about fraud during the course of their duties, it puts senior managers on notice that oversight isn't limited to the rank and file. And there's always the chance that one of the accomplices will report suspicious activities.

*Setting up a confidential tip hotline can help create an environment of vigilance.*

Periodic surprise audits, too, can dissuade upper management from acting on any fraud impulses. While such audits can't be comprehensive, they can serve as spot checks in high-risk areas such as inventory, sales and accounts receivable. They also can be




powerful deterrents to artificial asset inflations or other financial statement falsifications.

Lastly, if you find fraud, punish it. Nearly 40% of certified fraud examiners who responded to the *2005 Report on Corporate Fraud* sponsored by Oversight Systems said that prosecuting employees who commit fraud would greatly reduce domestic institutional fraud.

### Let fear deter

Too often, companies worried about the effects of adverse publicity wrap up their fraud investigations with only threats and beefed-up damage control efforts. That does little to convince would-be fraudsters that their activities will bring more pain than gain. In fact, it serves to demonstrate that your company basically turns a blind eye to crime — and that employees can steal with impunity.

Fraud is a risk that can have catastrophic consequences. Send a loud and clear message that fraud will be detected and punished, and you may find you've diminished your risk significantly. 

# How computer forensics experts snare evidence

It's every company's nightmare: An employee leaves, taking trade secrets to a new job. The rival company insists its products are the result of its own research and development, and you fear you have no way to prove otherwise.

Or do you? Enter the computer forensics specialist. Computer forensic techniques often play a role in fraud investigations, including embezzlement and theft of trade secrets. No matter how adept your former employee is at hiding evidence of fraud, a knowledgeable forensics expert is likely to find a computer trail. More important, the expert can preserve and protect it so it will stand up in court.

## No paper chase

In many ways, computer evidence is different from paper evidence. It comes in a variety of forms, including earlier versions that may still be on disks, or in alternate, hidden formats. It may have been deleted, encrypted or damaged.

The good news is that a computer forensics specialist often can access information without compromising it or allowing a virus to corrupt it. In most cases, the expert can minimize disruption to your business while information is being retrieved.

Equally important, these experts know where to look for evidence outside the perpetrator's computer. System logs, printouts, proxy server and firewall logs, notes jotted in manuals, and even what's physically on a monitor can prove just as valuable as what's recovered from hard drives, floppy disks and tapes.

## The process

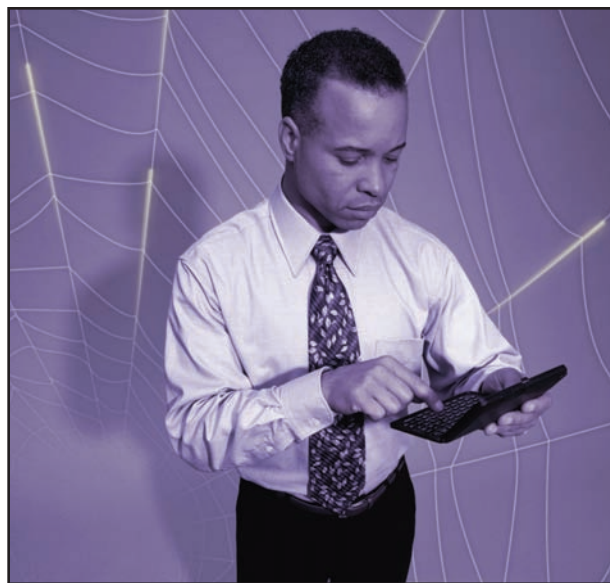
Typically, an expert will first secure your system against damage or corruption and then get to work on unearthing and extracting all files, including those the user thought had been deleted, or had password-protected. The specialist might have to recover hidden and deleted files, as well as those the computer's operating system or applications used as temporary or swap files.

An expert looks for data in areas of the hard drive that are typically inaccessible, including "unallocated" space on a disk (unused space that could previously have stored data) and "slack" space on a file (a blank

remnant at the end of a file that could previously have been used).

What the specialist does with the data found is just as important as finding it in the first place. A good computer forensics specialist approaches every analysis with the expectation that evidence will be required in court. Thus, every step of the analysis and every piece of potential evidence recovered is documented to prove the chain of custody and meet rules of evidence requirements.

As part of the documentation, the expert will provide an opinion on his or her findings. This report typically explains system layout, file structures and similar operational arrangements. If applicable, it also will discuss any evidence that shows the employee attempted to hide, delete, protect or encrypt files.



## Close the case

Combined with his or her expert consultation or testimony, the evidence that a computer forensics specialist can collect may be just what you need to close a case on trade secret theft — or any other occupational fraud.

But to ensure your computer forensics expert can find the smoking gun, engage one as soon as you suspect something is amiss. Attempting to retrieve files yourself could fatally disrupt the chain of custody or even destroy evidence. 🕒

# Don't get pinched

## Watch expense accounts for signs of cheating

With energy prices, inflation and consumer debt on the rise, more employees may be tempted to put unauthorized expenses on their expense accounts. Unfortunately, many employees and their managers view cheating on expense accounts in much the same way they view cheating on taxes: Everyone does it, and it doesn't cause any real harm unless it gets out of control.

The truth is that if “everyone does it” — even if it's just in small increments — it can add up to a whole lot of money. While you may understand the temptation, you shouldn't condone it. Instead, develop a sensible expense account policy and actively let employees know you'll be monitoring their expense reports for inflated amounts and larger-scale fraud.



### Recognize red flags

Most employees who cheat on their expense accounts do it in one of four ways:

1. Mischaracterizing expenses, in which they present legitimate documentation for nonbusiness expenses,
2. Overstating expenses,
3. Claiming fictitious expenses, or submitting fake receipts or bills, or
4. Requesting multiple reimbursements, or copying receipts or invoices and submitting them for more than one payment.

*An important component of any expense account policy is to prohibit photocopied receipts and invoices.*

The majority of false claims, however they are submitted, are related to travel and meals. Someone may, for example, collect a stack of taxicab receipts and periodically turn them in for fictitious reimbursements. The practice of treating friends or spouses to meals on the company dime has become so common that the term “business dinner” is often accompanied by a wink and a nod. And some employees are adept at getting reimbursed for a single credit-card expense two or three times, using the receipt, the statement and the bill for multiple expense account submissions.

### Nipping it in the bud

There are steps you can take to prevent expense account fraud from happening in the first place. First and foremost, review your policies to be sure they're reasonable and fair. Employees are more tempted to cheat when policies are so restrictive that they don't cover their out-of-pocket business expenses.

If you don't think a detailed expense policy is necessary, consider giving employees who travel flat-fee allocations that will cover all expenses. If you do that, set the limit high enough so your employees won't


run short. Also provide a means for them to submit additional expenses if they feel they're justified.

An important component of any expense account policy is to prohibit photocopied receipts and invoices. Photocopies frequently are used to disguise altered originals, and it isn't unreasonable to ask employees to submit original documentation. Be sure, however, that your policy has a mechanism by which employees may



request exceptions. Also require your supervisors to approve all expense reports, and periodically review those reports with an eye toward spotting unhealthy trends such as steadily increasing reimbursement claims or unreasonable charges.

### **Fairness and vigilance**

Everyone's likely to be feeling the pinch these days, but that's no reason for employers to let themselves get wrung dry. With a little extra vigilance and a visible, fair policy, you can keep expense account reimbursements under control. 



## **raud to watch for: Domain name registration scams**

Internet domain name scams have enjoyed renewed success among scam artists recently. Fraudsters use legitimate, publicly accessible databases to compile lists of businesses whose domain names are coming up for renewal. Then, in a scheme borrowed from the books of telephone "slammers" of the 1990s, the scammers send official-looking domain expiration notices that solicit payment to ensure the companies retain their Web addresses.

The problem isn't just that the requested payments are significantly higher than the nominal fee required for legitimate domain name renewal, but that businesses also unwittingly give authorization to transfer their domain name to a different registration company. You may not pay the legitimate renewal fee, and your domain name becomes available to someone else.

### **Dubious protection**

Alternatively, fraudulent domain name operators may claim to have been approached by other companies that want to register domain names similar to yours. In this case, the scam artist might offer to register your business with an ".info" or ".biz"

extension to protect it from identity theft and its name from other unscrupulous uses.

Yet another, highly successful, scheme is perpetrated by companies that offer domain name registration for very little (less than \$5 per year). When they've amassed thousands of customers, they sell their client bases to the highest bidders. Those bidders then send bills of up to \$50 for domain name registration renewals. The renewal notices are timed to arrive too late for the targets to transfer their registrations to reputable firms, meaning you could be forced either to stay with the unscrupulous company for another year or risk losing your domain name.

### **Educate employees**

IT professionals in most companies are aware of these types of scams, but it can be costly for you if other employees who are allowed to authorize small payments don't know about them. So inform your employees about domain name scammers; it may help preserve your good name.



# McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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



Craig L. Greene, CFE, CPA

An internationally recognized public speaker, Craig has lectured on topics involving fraud and its detection to auditors, investigators and attorneys. He is a faculty member of the Association of Certified Fraud Examiners and Institute of Internal Auditors.

Craig works as a consultant and expert witness for major corporations, law firms, law enforcement and governmental agencies on cases involving allegations of fraud and misrepresentation. Craig is frequently quoted in major newspapers and publications throughout the U.S.

**We welcome the opportunity to discuss your needs and answer any questions you might have about our fraud examination and litigation services.**

Please contact us at 312.419.1961 or visit us at [www.mcgovernngreene.com](http://www.mcgovernngreene.com) and let us know how we can be of assistance.

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

