Forensic Focus

Insights on fraud detection and deterrence

AUGUST/SEPTEMBER 2008

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

105 W. Madison Street • Suite 406 • Chicago, IL 60602
www.mcgoverngreene.com

Stop surprise deliveries

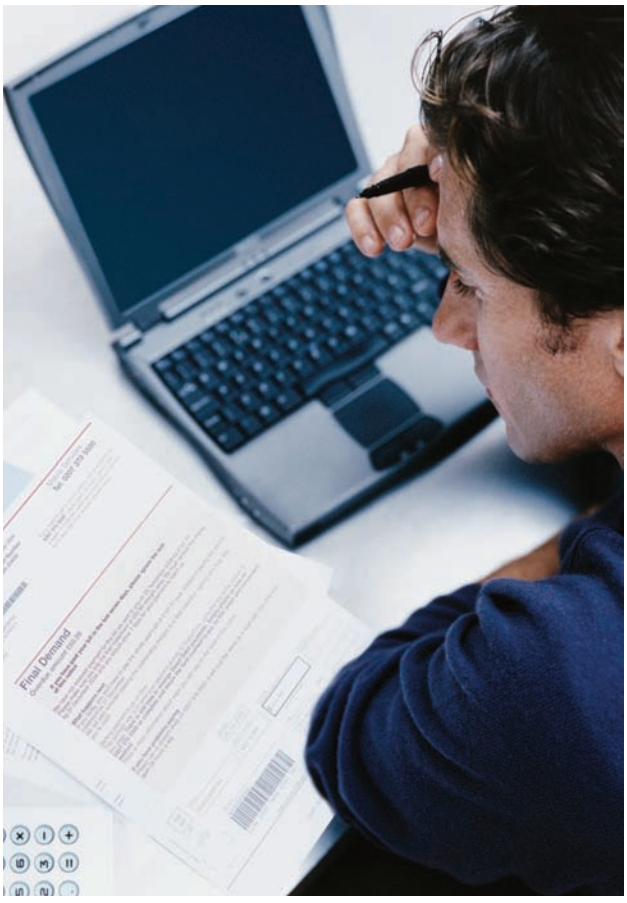
Recognizing and preventing office supply scams

As a business owner, you know the value of a good deal. Fraud artists, too, understand the appeal of money-saving offers, which is why they're working overtime to dupe your employees with phony office supply offers.

Office supply scams aren't new, but they're enduring. The Federal Trade Commission estimates they cost American businesses as much as $200 million a year. Fortune 500 companies aren't immune, but small businesses and nonprofit organizations are the most common targets.

Scams have staying power

Although supply scams vary, all have a few common features. They require the thief to gather information about your business in advance, and they depend on confusion and a lack of preparation on your end.



The scam typically begins as telemarketing fraud, with someone calling your business to obtain your street address and the name of an employee. The caller may ask for the person in charge of your Yellow Pages advertising, claim to need information to complete an order or pretend to verify your copy machine's serial number. The goal is to get a name that will lend legitimacy to the bogus invoices or shoddy products the fraudster is preparing to send you.

Sometimes, scam artists don't even go to the trouble of shipping products.

Watch out for phony invoices

After the caller has the information, he or she may try one of several common scams. For example, the thief may ship poor quality products, and then follow up a week or two later with an exceptionally pricey invoice. The delay is intentional: He or she is hoping you won't notice that the final price is much higher than you'd pay for better quality products from a legitimate supplier. The fraudster is also hoping that you will have used some of the products and feel obligated to pay for them.

Sometimes, scam artists don't even go to the trouble of shipping products. Instead, they just send phony invoices timed to arrive when you would normally receive a bill for a purchase from a real supplier. You could, for example, receive a phony invoice for advertising shortly after your actual ad runs in a publication.

Be wary of pretenders

Some fraudsters — "toner phoners" are among the most notorious — want to restock your existing supplies. They pretend to be "authorized" dealers, or previous suppliers, and offer to send you replacement ink toner for your copy machines, light bulbs or other supplies.

Even though they're happy to discuss, for example, how many cartons you'll need, they're less eager to talk about price or brand names. When pressed, they may say the price hasn't changed since the last time you ordered, or that the price is $20 in a carton of 10. You should beware of either, but the latter should really set your fraud alert antennae quivering. It likely means each carton will end up costing you $200.

Sometimes pretenders don't offer to sell you anything. Instead, they'll offer to send you a promotional item. Before they hang up, however, they'll mention in passing that they are going to throw some ink cartridges in with the free coffee mug. What they don't mention is that they'll also throw in a bill for the ink.

Refuse gift horses

The "gift horse" scam is a common ploy that works by pitting you against an employee. The fraudster sends a promotional item to an employee, and follows up by sending unordered merchandise to you. When you receive the bill with the employee's name on it, you question the employee.

The scammer is hoping the employee will be so nervous about accepting the promotional item that you'll end up believing he or she mistakenly ordered the additional merchandise. The fake supplier also hopes, of course, that you'll pay for it.

Lines of defense

Scam artists will dog you until you pay, and once you do, they'll send subsequent shipments to begin the cycle again. So the best way to stop office supply scams is not to let them begin.

Your first line of defense is the employees who answer your phones. Give them an out by designating one or more buyers to whom they can refer all telemarketing calls. Then, when someone calls to offer two-for-one toilet paper, whoever answers the phone can politely say that all purchasing is done through your buyers.

Next, establish procedures for your buyers to follow, including how orders are to be documented and approved. Set up a system for generating purchase order or internal reference numbers and ask your vendors to include those numbers on their shipment documents. When buyers make purchases, they should forward copies of their orders to accounts payable.

When you receive merchandise, inspect it. Using your reference numbers, verify that you ordered it and ensure that packing lists match what's in the boxes. If everything's in order, the receiving employees should send copies of the bills of lading to accounts payable for reconciliation with the order.

According to the law ...

You aren't legally required to pay for anything you didn't order; nor are you required to return it. Unless there's a legitimate mistake on an order, you may treat any unrequested merchandise as a gift and use it — or toss it — as you like.

If suppliers continue to hassle you, discuss the matter with your legal and accounting advisors. They can help you decide if it's a matter for the police and criminal prosecutors.

Savvy shopping

Legitimate companies do offer specials on office supplies, and you should certainly take advantage of them. But it's always a good idea to know your vendors and establish that they're legitimate businesses before you accept their supply shipments or gifts — or pay their invoices. ■

Soft-hearted *and* hard-headed

How to avoid charitable fraud schemes

Businesses are frequently asked to donate money or goods to charity. Nine times out of 10 such requests are legitimate and your only problem is deciding how to allocate your charitable dollars. It's the tenth one that can cause you grief. Fraudulent operators will do whatever it takes to get their hands on your company's money, and they're more than willing to appeal to your generosity.

Advertising scams

In one common charity scam, fraudsters call and ask your company to renew an ad in a publication purporting to be associated with your local police or fire department. Such publications do exist, but the scam artists aren't associated with them, and you've never advertised in them. The employee answering the phone doesn't likely know that.

You can avoid being taken if you learn to recognize some warning signs. The "salesperson," for example, won't give you a price unless you ask, and he or she may not be eager to discuss the publication's distribution area. That's because the publication doesn't exist. In some cases, you might receive an actual ad in return for your donation, but the publication may go only to a small group of people far outside your community.

Book covers and placemats are other tools scam artists use to dupe businesses. They may say they're collecting money to design book covers with anti-drug or antiviolence messages for distribution in the local high school. Or they may claim to be printing Earth Day information on placemats for a local food co-op's vegetarian chili supper. The problem is that the high school and food co-op have no association with the printing company and will never see the material you paid for.

Protecting yourself

Before you donate a dime, get the full name and address of the organization and the names of its principal officers. Many states require charitable organizations to register before they solicit in that state. The offices vary — in Illinois, it's the Attorney General's office; in Wisconsin, the Department of Regulation and Licensing.

If someone is trying to sell you advertising, ask to see a copy of the most recent publication. Then probe further by asking:

- When the next issue will be published,
- Where it will be distributed,
- How many copies will be produced, and
- Who the target audience is, including any demographic information that's available.

If the solicitor doesn't have the answers, be wary. And don't allow yourself to be rushed. Get the person's name and contact information and promise to get back to him or her after you've had time to consider. A legitimate salesperson will be willing to wait a few days.

Speak up

If you believe you've been approached by a scam artist, speak up. Notify the state office that regulates charitable organizations, and drop a tip to your local newspaper. Fraudulent charities don't want to be in the public spotlight. If you can put them there, they'll disappear pretty quickly. Unfortunately, they may come back in a new guise. ■

Are your employees flying the red flags of fraud?

As an owner, you're your company's first line of defense in spotting fraud. A forensic accountant may be the best person to unearth the "hows and whys" of a theft, but it's up to you to know when it's time to call in professional help. The signs can be easy to miss, but they're usually there.

When something doesn't belong

Fraudsters may use anything from fictitious vendors to false invoices to cover their tracks. Look for duplicate payments, out-of-sequence entries, differences in handwriting, entries by employees who don't usually make them and accounts that don't properly balance.

Scan transactions for amounts that appear too large or too small, as well as those that occur too often or too rarely. And if no one can explain an unusual journal entry or adjustments to inventory or accounts receivable, it merits further investigation.

An increase in the number of complaints your company receives is another warning sign. An investigation may lead to a relatively innocent cause, such as a glitch in your shipping system — or it may lead to a fraudulent billing scheme. Pay equally close attention to declines in product quality. They could just stem from a faulty batch of paint, or they may indicate that a fraudster is working in your purchasing department.

Look for la vida loca

Changes in an employee's lifestyle may be evidence of fraud. Few thieves, after all, steal to save the money. Lifestyle changes can be difficult to spot, at least initially, but over time a pattern is likely to emerge.

One piece of expensive jewelry could be a gift, and a good return on an investment may be the impetus for an exotic vacation. But if your warehouse manager starts wearing a new pair of expensive shoes

every day, buys a boat and installs a backyard pool, you may have to question how that's possible on the salary you're paying. In short, if someone's ship seems to have come in, ask where it's docked.

Besetting sins

When employees steal, especially if they're first-time offenders, they may no longer be on their best behavior. In fact, you may not even recognize them. People who have always been cooperative may become argumentative. Or, alternatively, someone who typically has been difficult to work with may suddenly become everyone's friend.

If an employee starts drinking to excess or takes up smoking, ask what's wrong. If they can't sleep, worry obsessively about the possible consequences of actions, resent other employees' participation in "their" projects or even just sweat a lot, be concerned. They may be wrestling with a personal problem such as divorce, or they may be stealing you blind.

Don't jump to conclusions

The signs of fraud are easy to overlook, in part because they aren't necessarily signs of fraud. There may be logical, acceptable and reasonable explanations for suspicious behavior, but you won't know unless you ask. And once you ask, don't stop until you're satisfied with the answers. ■

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, decide 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.

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 police in either event.

Change with the times

After you've created and implemented your fraud contingency plan, review it regularly because change — such as employee turnover and new suppliers and products — is a constant 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. ■

Enlist the IRS in your fight against fraud

You thought you could trust your employees, but now someone has embezzled from your company. And even though you're sure you know who did it, neither you nor the police can prove it. So you're stuck, right?

Not necessarily. You may find an unlikely ally in the IRS.

Income is income

It's a pretty safe bet that the embezzler failed to report his or her extra "income" to Uncle Sam. And the IRS certainly will be interested in prosecuting the individual for tax evasion — regardless of whether a fraud prosecution can be mounted. Federal income tax authorities aren't as concerned with the source of people's money as with whether they paid income tax on it.

You'll enjoy another benefit by getting the IRS involved: If caught, the thief will be punished and you may be able to deduct the amount that was embezzled from your company's taxes. Of course, that may not be as easy as it sounds. Reporting the embezzlement to the IRS is one way to document your loss, but you'll also need to report it to the police if you want to establish that you were a victim of theft. Losses due to theft are deductible in the year in which they're discovered, regardless of when they occurred.

Your strongest substantiation for a theft deduction will be the employee's criminal conviction, but you may also use reasonable inferences that point to theft. If, for example, you discover the embezzlement around the time your suspect employee buys a luxury car you know he or she can't afford, there may be a reasonable inference that a crime has been committed.

The support you need

If you can convince tax authorities that your money was stolen and you have little chance of recovering any of it, you can deduct the full amount from your company's taxes. But keep in mind that, if you underestimate the amount you may recover, the IRS will treat anything you receive over that amount as taxable income.

Before approaching the IRS about possible fraud, consult your tax professional and attorney about the best way to enlist the government's help. Income tax is complicated, even when it's clear you're the victim.

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

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

CRAIG L. GREENE, CPA, CFE, MCJ

Craig is a leading fraud examiner and white collar criminologist. With over 30 years of experience, he frequently testifies in cases involving financial fraud, accounting, audit, and other disputes involving financial issues. Craig has led many corporate internal investigations focusing on financial statement fraud, corrupt payments, embezzlement and other occupational fraud schemes. He is an international lecturer on forensic accounting and fraud examination issues. E-mail: craig.greene@mcgoverngreene.com

CONTACT US AT 312.419.1961 OR VISIT www.mcgoverngreene.com
FOR EXPERT FRAUD EXAMINATION AND LITIGATION SERVICES

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