

fraud alert

february/march 2006

Scene of the crime

**How to preserve
fraud evidence**

**Procurement fraud:
When purchasing costs
more than it should**

**Is organized crime
harming your business?**

**Medicare Part D
benefits fraudsters, too**

**Fraud to watch for:
Phantom regulators**



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

Scene of the crime

How to preserve fraud evidence

What's the first thing you should do if you discover your business has become a victim of fraud? Fix it and get back to work, right?

Not so fast. The first action you should take when you find evidence of fraudulent activity (after contacting your attorney) is to preserve evidence. Too often, in their haste to get back to business as usual, companies neglect to think about the data they might be destroying or discarding as they reset computer systems and clean out desks.

Without evidence, fraud can't be fully traced and perpetrators can't be prosecuted and punished. Remember that it's in a fraudster's best interest to destroy anything that could implicate him- or herself, especially if the fraud you've spotted is just one piece of a bigger scam.

Preserve paper

Place anything you find in a safe location that's accessible only to key people. The fewer people who handle it, the better — a consideration to keep in mind not only when storing documentation but also when collecting it. Don't make notes on any paper documents and, unless necessary, don't let them be handled. Instead, make separate notations about when and where they were found and how you preserved them. A court case can be derailed if you don't preserve the chain of evidence and can't prove to a judge's satisfaction that the documents haven't been tampered with.

Handling paper documents is relatively easy as long as you approach the task with care. You can copy anything you need to continue operations, and turn the originals over to fraud examiners or law enforcement for fingerprinting, handwriting analysis or other forensic testing.

Tackle technology

Computers can be another story, especially if your internal information technology (IT) staff isn't trained to deal with fraud evidence. IT personnel may be highly skilled at setting up and troubleshooting your computer applications, but they're unlikely to be fully aware of the legal ramifications of having one of your company's computers used for fraud.

Even the most skilled IT technician may unintentionally alter or destroy computer evidence in the course

of restoring the computer to normal operations. To avoid such mishaps, train your staff how to respond to incidents of fraud. Training should emphasize that the first requirement is to stop any routine data destruction immediately. If your system automatically deletes certain information — including e-mails — every couple of months, that process must be discontinued the minute you learn something is amiss.

The training also should include a realistic assessment of your staff's strengths and capabilities, as well as their limitations. If no one on your staff has a background in computer forensics, they should keep their investigative activities to a minimum while they act promptly to ensure that no further alterations can be made to existing files.



Cyberforensic specialists can identify and restore altered records, digital forgeries and files that have been intentionally corrupted. They also can get to secured or password-protected files and pinpoint unauthorized system access — all without destroying or damaging the suspect files.

Be prepared

Successful fraud investigations rise or fall on the amount and integrity of the evidence that is uncovered. Preparing to respond in a manner that preserves fraud evidence is the first step in the process of catching and punishing a thief. ❏

Procurement fraud: When purchasing costs more than it should

You spend time searching for high-quality products at the lowest available price. Do you spend the same amount of time assuring yourself that you're getting what you're paying for?

Procurement fraud is pervasive in businesses, whether by fraudulent vendors, a company's own staff, or both. Kickbacks, fictitious vendors, short deliveries, and a host of other scams are perpetrated through purchasing departments more often than you might think.

Words to the wise

When procurement fraud involves cash payments to employees, it can be difficult to detect because those payments aren't reflected in your books. They probably are, however, reflected in higher pricing. Even fraudulent vendors must cover their costs, after all.

If you find you're paying higher prices for lower quality, you may simply be a victim of marketplace fluctuations. But it's worth taking a closer look at your procurement practices. Signs that something is amiss may be consistent shortages, informal communication (such as cell phone calls or personal e-mails) between your purchasing staff and suppliers, and poor record-keeping.

As with any type of fraud, the best way to avoid procurement department problems is to develop policies and take other preventive steps.



Other places to look

The most common procurement fraud involves payments to fictitious companies. Photocopied invoices, sequentially numbered invoices from a single vendor, invoices from companies that have only post-office box addresses and invoice amounts that are consistently just below sums that must be approved for payment are warnings that procurement fraud is occurring.

Look, too, for connections between your procurement staff and your suppliers. Is one of your employees related to or otherwise linked with the owner or management of a supplier? If so, that employee shouldn't be making purchasing decisions that involve that company. Also, don't allow one employee to handle most or all of the purchasing procedures. The person who orders supplies and materials, for example, shouldn't be the same one who checks in shipments or approves invoices.

Prevention is the best medicine

As with any type of fraud, the best way to avoid procurement department problems is to develop policies

and take other preventive steps. Consider implementing these measures:

Develop a code of ethics. Define the standards by which you expect your employees — and your vendors — to conduct business, and communicate them in writing. Review and update the standards annually, and ask employees and vendors to sign them every year, even if nothing changes. It will refresh their memories and reinforce the importance you place on ethical, professional business practices.

Set up a hotline. Establish an anonymous fraud hotline. Better yet, establish two: one for employees and a separate one for vendors to report any suspicious or questionable activities. Giving vendors a separate line makes them more comfortable sharing concerns, and allows you to field any questions they may have about your standards for ethical practices.

Qualify vendors. Background checks that give you information on your vendors' affiliations, ownership, litigation, regulatory or legal violations or suspensions, and financial standing can help you weed out those with dubious histories. If you receive such information from the vendor, it's wise to verify it, at least with spot checks.



Contracts can breed fraud

If your business involves contract bids for goods or services, you carry additional fraud risk. One risk is that the person who approves those contracts is also receiving kickbacks from vendors.

Kickback recipients steer bids to their preferred company. In doing so, they may leave evidence of their activities, for example:


- A scarcity of qualified bids, suggesting competition wasn't actively sought,
- Narrow bid requirements, which may indicate specs were tailored to a particular company,
- Moving deadlines, suggesting a preferred contractor was outbid or didn't complete its proposal on time,
- Poorly drafted bid solicitations, indicating an effort to leave some room to maneuver in awarding the bids, and
- Outside help in writing specifications which provide an opportunity for current vendors to insert their own practices or products into future bids, thereby curtailing competition.

Contract fraud can be subtle, but it potentially damages your company financially and your business's reputation in the industry. If your procurement practices routinely involve deadline changes, don't draw as many bids as you would expect or attract widely divergent bids on the same projects, look more closely at your bidding policies. What you find may surprise you.

Review your records. Periodically conduct random checks of your business records. Look for vendor address and telephone matches that could indicate two purportedly different companies are, in fact, the same or related. Also look for proof that supplies or services were delivered as ordered and that there are no billing and payment anomalies in amounts, invoice numbering or other red-flag areas.

Each of these approaches, along with establishing appropriate oversight in areas such as receiving and authorization, can help you control fraud by putting employees and vendors alike on notice that fraud will not be tolerated and will be detected.

Guard your reputation

Procurement and purchasing present virtually limitless opportunities for fraudsters. You can mitigate your company's fraud risk by being aware of opportunities and vigilant in maintaining procedures and practices that will prevent or expose fraud. Develop a reputation as a reputable business and would-be perpetrators may just go where it's easier for them to operate. 

Is organized crime harming your business?

When most people think of organized crime, they think of drugs, prostitution, gambling and other unsavory activities conducted in a murky underworld — one that doesn't affect them. And in one sense, they're right.

But organized crime is involved in other activities that lead to diminished competition, reduced wages and higher costs, all of which affect legitimate businesses. These criminals have a long history of infiltrating companies to control unions, employee benefit plans and contract allocation.

Ripples reach far

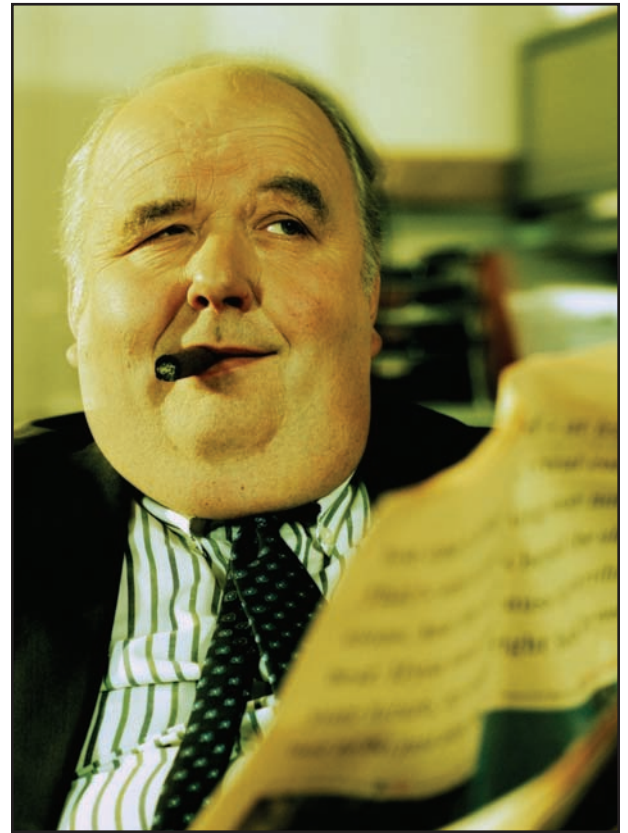
Much of organized crime's labor racketeering efforts have been concentrated in unions, but there is a ripple effect that touches politics, financial markets, major industries and, in some cases, individual businesses. The Office of Inspector General (OIG) had 130 open labor racketeering cases that involved organized crime between October 2003 and September 2004 (the latest available figures). Of those, half involved pensions and employee welfare benefit plans.

Shady benefits service providers are particularly alarming, because they can cause substantial financial losses by affecting multiple plans. Plus, they're sophisticated enough to conceal their activities through complex financial machinations.

Unfortunately, it's difficult for legitimate employers to tell when their providers aren't on the up-and-up. If something doesn't ring true, however, talk to a trusted financial advisor to learn more about how things are supposed to work. A plan administrator who is evasive or can't easily answer questions about the plan, for example, or an account that doesn't appear to be performing to your expectations merits closer attention. Even if such concerns are unrelated to organized crime, they should be addressed and, if necessary, corrected.

New and different approaches

Organized crime is also having an impact on global business. Nontraditional, ethnic gangs are emerging to join with — or replace — more established networks. These newer players organize retail shoplifting rings to steal high-value items for resale or sell counterfeit versions of everyday products. In 2004, authorities seized 34 million counterfeit



batteries, 31 million bogus shaving products and thousands of toothbrushes, purportedly manufactured by the Gillette Company — contraband Gillette estimates created a \$200 billion loss to the economy.

But catching these criminals is difficult. Organized crime takes pains to remain invisible while it affects legitimate businesses. Businesses, in turn, may not be aware that organized crime is part of the reason the cost of their benefits is rising, or they aren't winning contracts they expect to get. In the case of shoplifting rings, perpetrators often are prosecuted as shoplifters, leaving the real leaders and organization behind them untouched.

The fight goes on

Federal authorities, though, are well aware of the influence organized crime wields. In recent years, as FBI resources have increasingly been diverted to antiterrorism efforts, the OIG has taken a more prominent role in combating organized crime. For more information, or to report suspicious activities, visit the FBI's Web site at www.fbi.gov, or the OIG's site at www.oig.dol.gov.

Medicare Part D benefits fraudsters, too

As employers, health care providers, insurers and senior citizens across the country geared up for the Jan. 1 launch of Medicare Part D prescription drug benefits, they weren't thinking about fraud. Others were, though. While the health care and pharmaceutical industries raced to understand, explain and implement this challenging new component of the nation's health benefits, fraud perpetrators were targeting retirees with telemarketing scams and finding other ways to profit from government benefits designed to help, not hurt, patients.

Confusion = opportunity

Medicare Part D represents a major change in benefits that are available for Medicare and Medicaid patients. But the rules governing that change are complex at best and virtually incomprehensible at worst, particularly for beneficiaries. This provides an opportunity for scam artists.

Senior citizens have reported receiving calls offering assistance in enrolling in Part D, or claiming their Medicare cards would soon expire. Callers have requested personal information such as bank account or credit card numbers as part of their "assistance."

Of course, Medicare beneficiaries have been bombarded with calls and mailings from legitimate providers vying for their business. More than 10 companies are offering competing plans with varying coverage options in every state. And residents of some states have nearly 50 from which to choose.

Employers can help their retirees sort through the tangle by renewing antifraud educational efforts, and by making staff available to answer questions about various plans — taking care not to recommend one over another — or referring retirees to the Medicare information line (1-800-MEDICARE) or Web site (www.medicare.gov).

Drug company woes

The confusion, coupled with the disarray surrounding the launch of any ambitious undertaking, leaves the

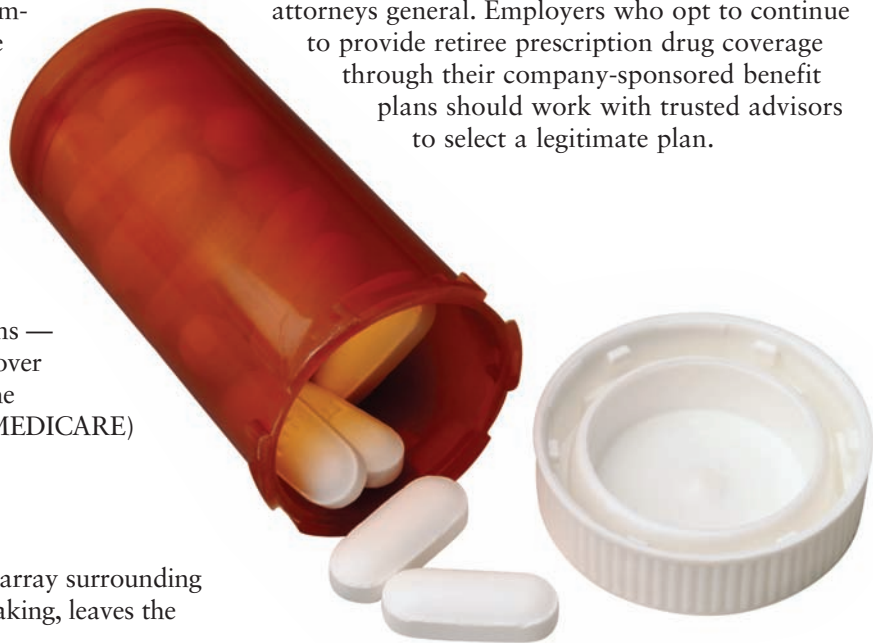
door open not only to telemarketing fraud but also to expansions of the illicit operations that have plagued the pharmaceutical industry in recent years.

Fraudulent pricing and marketing of cancer drugs, sale of counterfeit AIDS medications, and online sales of discount "Canadian" drugs all have resulted in millions of dollars in ill-gotten earnings since 2003. That doesn't include the more than \$2.4 billion recovered from drug manufacturers as a result of false claims against Medicare and Medicaid, as reported by the Taxpayers Against Fraud Education Fund in 2004.

Practice vigilance

It's unlikely Medicare Part D will reduce those false claims. Inflated prices, bogus prescriptions and the like aren't products of how drugs are prescribed or distributed or even who pays for them. They're the products of opportunity, seized by people with agile minds and the ability to keep rewriting their programs.

What then, can employers and patients do to protect themselves? As with any potential fraud, no one should give personal information to unsolicited callers. Better yet, check callers' bona fides: if the call is allegedly from a bank or police department, hang up and call the bank or department. If the call wasn't legitimate, it should be reported to state attorneys general. Employers who opt to continue to provide retiree prescription drug coverage through their company-sponsored benefit plans should work with trusted advisors to select a legitimate plan.



Help is available

Employers can get some assistance from Medicare's Web site. Another government site, www.cms.hhs.gov, offers a state-by-state breakdown of available plans. Also, although Medicare Part D benefits went into effect Jan. 1, open enrollment in the program continues through May 15. A short delay in enrollment may give seniors and their former employers an

opportunity to evaluate various plans after they've been in operation for a few months.

Beneficiaries can't delay too long, though. After May 15, those who don't have prescription drug coverage through an employer-provided plan must pay a penalty for late enrollment. ❗



fraud to watch for: Phantom regulators

In a new twist on an old fraud, con artists are posing as securities regulators to persuade investors to buy worthless securities or pay "transaction taxes." Officials in Massachusetts, Missouri, Montana and New Jersey have all uncovered these types of scams, which they say are only the tip of what could be a very large iceberg.

The con

Typically, phantom regulators obtain information about investors' holdings (regulators are still trying to discover how), and then contact them, offering to pay premium prices for the stock. In exchange, victims pay what the con artists claim are security bonds or transaction taxes. When cautious investors have questions, they're referred to bogus protection or trade services that authenticate the sham regulators. Their suspicions allayed, investors send payments to U.S. bank accounts from which the money is transferred overseas to the fraud perpetrators.

In other cases, phantom regulators use legitimate-looking Web sites to get investors to buy worthless securities from unlicensed brokers.

Signs of trouble

According to the North American Securities Administrators Association (NASAA), there are five significant signs regulators aren't legitimate:

1. No other legitimate regulatory Web site, such as the International Organization of Securities

Commissions' www.iosco.org, includes references to them.

2. They endorse opportunities or businesses. Real regulators are involved only in enforcing the law.
3. They contend that fees to "release restricted shares" are legitimate.
4. Internet search engines turn up little or no information on them.
5. Other regulators say they've never heard of them.



State and federal officials are investigating reports of phantom regulators, and are circulating tips and information about them to help alert the public. To date, officials have identified a number of fake regulators investors should be wary of, including the Regulatory

Compliance Commission, the International Regulatory Commission and the International Compliance Commission.

The best defense

Still, the best defense for investors is common sense. No matter how good or legitimate a deal may seem, if it was unsolicited, talk to a trusted financial advisor before accepting it.

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 and let us know how we can be of assistance.

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

