Forensic Focus

Insights on fraud detection and deterrence

JUNE/JULY 2008

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

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

E-procurement

Are you taking advantage of this automated fraud detector?

If you've purchased an e-procurement system, you're likely thrilled with the way it has standardized procurement processes across all departments. You no longer need as many people to place, process and pay for orders, and you're probably seeing significant cost savings.

But if you're not using the system to prevent and detect fraud, you may not be getting your money's worth. As automated procurement systems become more sophisticated, they're being used to process ever larger numbers of transactions. And, no matter how well you've designed and implemented controls, there's always a way for motivated thieves to work around them.

Old methods lacking

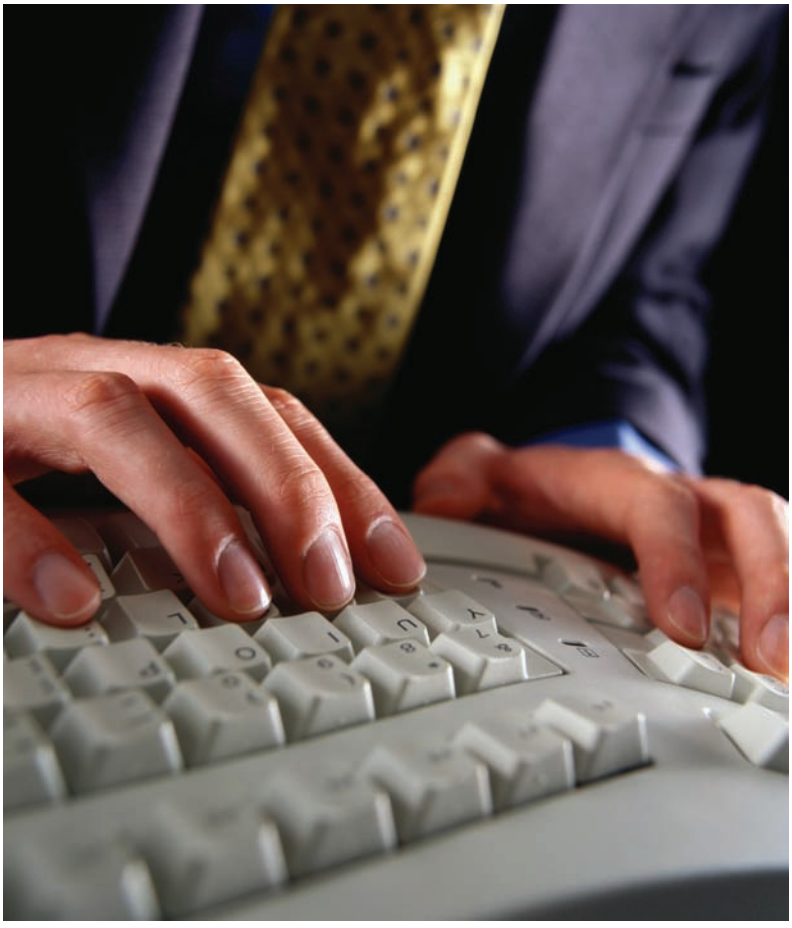
Many organizations manually review invoices for possible fraud. But this is unlikely to be very effective, because auditors can overlook potentially fraudulent transactions after viewing so many legitimate records. Sampling is an option, but the sample size required to ensure a reasonable chance of spotting fraud often is too large to be feasible.

The good news is that an e-procurement system can be just as efficient at spotting red flags for fraud as it is at moving your orders along. In one such examination, a large public school district in North Carolina discovered that payments to a certain vendor increased 342% in a single year, according to a 2006 report by audit resource sites EZ-R Stats and AuditNet. Two-thirds of the invoices to the vendor were under the district's $2,500 bid limit, and at least 50 of the vendor's invoices had the same date — many with consecutive invoice numbers. Employees behind the scheme used the pilfered funds to buy big-ticket personal items.

Set your parameters

An e-procurement system has fewer limitations than older screening methods. The number of transactions your system handles each day may make it impossible to monitor every single one, but you can set parameters to flag those at highest risk for fraud. Your system can scrutinize spending trends by supplier, employee or product.

And you can set your system to test for any conditions — including transactions that were



approved against policy — and to identify unusual patterns and trends that suggest fraud is occurring.

You might, for example, look for payments made during a specific month to vendors who receive annual payments of $10,000 or more. By charting the number and amounts of payments, you can spot spikes or other unusual patterns. Or if you match payments to purchase orders, you can identify payments that should have been made with purchase orders, but weren't.

Personal factors

Don't assume that your system will catch all fraudulent transactions. A good e-procurement system won't allow buyers to circumvent required approvals, but resourceful and determined employees bent on fraud can usually find ways that get around any system. That's why it's important to look for other fraud warning signs, such as employees who appear to live beyond their means.

Combine your screens with employee profiling to isolate potential problems before they become realities. For instance, transactions initiated by a new employee who has just purchased a luxury car could be monitored and flagged according to the risk level. If the employee has regular opportunities to misappropriate large sums, he or she would probably be considered a high risk for fraud. In this case, consider requiring that all transactions initiated by that individual be sent to a manager for final approval.

If you match payments to purchase orders, you can identify payments that should have been made with purchase orders, but weren't.

Depending on your software, you may be able to integrate travel and expense costs — which tend to be high fraud risk transactions — into your procurement system. Doing so will subject these items to additional authorizations and more stringent oversight.

Who commits procurement fraud?

It would be easy if fraud-perpetrating employees looked like the crooks they are. But they don't. That's because most employees charged with occupational fraud don't have criminal records: According to the Association of Certified Fraud Examiners' *2006 Report to the Nation*, nearly 90% haven't previously been charged or convicted of any fraud-related crime in the past.

The report also noted that billing (or procurement) schemes, which are the most common fraud and associated with the largest losses, are largely committed by accounting personnel or upper management. And sadly, the longer the person has been with a company and the higher his or her salary, the greater the median fraud loss. Men are twice as likely to commit fraud as women, and most fraudsters are 41- to 50-year-old employees or middle managers.

In other words, the most successful fraudsters are often the most reliable and valued workers. It may be hard to think of trusted employees as potential thieves, but you won't be wrong if you remember the maxim "trust, but verify."

Let it be known

Not only does your e-procurement system help identify fraud, but it also acts as a deterrent by notifying employees that their activities are being monitored. Of course, you shouldn't assume that every transaction that's flagged for your attention is fraudulent. Many discrepancies have perfectly reasonable explanations.

So be careful about making accusations or taking action without thoroughly considering the consequences. If you have strong evidence of fraud, consult an attorney and a forensic accountant before attempting to interview the potential perpetrator or retrieve evidence from his or her computer. (See "Leave the questions to the professionals" on page 5 for more information on interviewing potential fraudsters.) ■

Protecting your business from payroll fraud

Remember when someone who wanted to commit payroll fraud had to get his or her hands on an actual check? Today's fraudsters need only a computer — and even worse, you may be held responsible if they succeed in scamming your financial institution.

Computers make it easier

Criminals once used chemicals to alter stolen checks or invested in expensive printing equipment to create new checks that could pass banks' scrutiny. Now, with a computer and a little know-how, they can make checks in a few hours from their home computer.

And if these forged checks get past your bank, there's no guarantee the bank will be held liable for honoring invalid checks. Instead, because you're deemed the party in the best position to prevent the loss, you may also be left holding the entire bag of losses.

Encourage direct deposit

Fortunately, there are some ways to prevent payroll fraud from happening. One is to encourage your employees to use direct deposit. Not only is direct deposit more convenient — and free — for employees, but it also ensures that no one can cash a bogus check.

But for employers who hire workers without bank accounts, such as seasonal, migrant and recent immigrant workers, direct deposit hasn't been an option, until now. In recent years, banks seeking to reduce their fraud risk have begun offering "unbanked" employees direct deposit programs at their work sites. Rather than being deposited into a traditional bank account, paychecks are credited on an ATM card or paycard.

With direct deposit, employees are freed from the fees they pay to cash paychecks, banks mitigate their financial liability to fraud, and businesses offer an added benefit that helps attract and retain workers. In addition, your corporate payroll

account number is no longer distributed around check-cashing outlets, and you don't have the hassle and cost of distributing checks, replacing lost checks, and buying paper checks.

Sign them the old-fashioned way

If you can't eliminate paper checks entirely, try to limit the number of authorized check signers. And use a "positive pay" system that allows the bank to verify all the checks presented for payment on your account. Further, unless you're writing hundreds of payroll checks, don't use an automated signature. Real signatures are more difficult to forge.

You might also consider outsourcing your payroll processing. Not only can an outside payroll service save you time and money in calculating and issuing checks, but it moves the entire payroll process off site. This way, employees have fewer opportunities to falsify or forge a payroll check.

Fight back

Payroll check scammers are more sophisticated these days, but savvy business owners can fight technology with technology. The same advancements that have made check fraud easier for perpetrators may also help you prevent these scams. ■

Leave the questions to the professionals

Fraud interviews are best handled by fraud experts

When you suspect an employee of fraud, you may be tempted to bring that individual in for a good grilling. A better idea is to leave interrogations to the experts. Fraud specialists are more likely to be objective, and they know how to make the most of what may be their one opportunity to question a possible perpetrator.

At ease, please

So long as the questions posed are reasonable, employees have a duty to cooperate with an internal investigation. They're likely to be nervous, however, and a trained fraud investigator generally starts an interview session by attempting to put subjects at ease. In establishing rapport, the investigator can lessen an employee's anxiety and gain his or her cooperation.

The objective of a fraud interview is to discover motives and opportunities for malfeasance — whether the subject is the suspected fraudster or the suspect's co-workers. Experienced investigators prepare questions in advance and structure each interview to get as much information as possible. Rather than saying they suspect fraud, for example, investigators might say they're looking into how the company's cash management system is being administered. Open-ended questions encourage subjects to talk at length and not simply provide "yes" and "no" answers.

Trained investigators take note of body language, changes in the subject's tone of voice and other nonverbal clues to the employee's beliefs and level of honesty. Knowing that an individual must offer his or her assistance voluntarily, without coercion, and must be able to leave the session at any time, the interviewer takes care to avoid an accusatory or antagonistic tone. This is easier for an outsider who doesn't know the subjects and isn't emotionally involved in the investigation's outcome.

Building a case

Fraud professionals keep accurate written records of each interview to address conflicting or inconsistent stories and so that they can be used later in court. At the same time, the investigator recognizes that any records generated during the investigation may be subpoenaed, so he or she adheres to strict professional standards in creating and maintaining records.

Additionally, fraud investigators work closely with attorneys and other advisors and authorities. Experienced investigators understand the rules surrounding attorney-client privilege, for example, and may defer some interviews to an attorney if privilege could be an issue.

Lastly, these experts recognize that interviews are just one part of a fraud investigation. Although interviews are a critical component, investigators also rely heavily on the documentary evidence they gather — including financial records and the contents of employees' hard drives.

Avoid alienation

Professional fraud investigators can prepare and present compelling cases constructed of computer forensics, data analysis and interview evidence. Business owners untrained in fraud investigations who try to conduct interviews on their own may only intimidate and alienate employees and jeopardize any chance of prosecuting perpetrators. ■

Don't run afoul of SOX 806 whistleblower protections

The Sarbanes-Oxley Act (SOX) prohibits retaliation against employees who report suspicions of fraud. Although SOX rules apply primarily to public companies, private business owners should be familiar with the provisions of the whistleblower protection. Otherwise, you may find yourself in violation without even knowing it.

No hassles

SOX Section 806 prohibits publicly traded companies, including their officers, employees, contractors, subcontractors or agents, from discharging, demoting, suspending, threatening, or discriminating or retaliating against a whistleblower. This includes employees who have filed a complaint or participated in or assisted with a fraud investigation.

Yes, you might say, but my company isn't publicly traded, so SOX doesn't apply to me. Don't be so sure. In some cases, the Department of Labor (DOL) has held that private businesses have been acting as agents or subcontractors of public companies and are, thus, covered by SOX. Even if you have no dealings with publicly traded companies, today's regulatory climate suggests it's smart to try to abide by the same standards as your public counterparts.

Make absolutely certain all supervisors understand that retaliation isn't allowed if an employee's allegations become known.

Standard of proof

For employees reporting a retaliatory act, the standard of proof under SOX 806 isn't very high. They aren't required to prove fraud or even that their firing was retaliatory. Employees just need to show

that they reasonably believed a fraud was being perpetrated, that they disclosed that belief to their employer or to authorities, and that they were fired within a short time after the disclosure.

If an employee meets the standard of proof, the business must prove by clear and convincing evidence that it would have fired the employee regardless of the whistleblowing. That isn't always easy to do, and sometimes the DOL may order that the employee be reinstated before there's even a hearing on the merits of the claim.

Avoidance is the best policy

Your best bet is to avoid running afoul of SOX 806 in the first place. Be sure your employees understand how they can report suspicious activity without fear of reprisal by, for example, calling your confidential hotline. Also make absolutely certain all supervisors understand that retaliation isn't allowed.

As part of your fraud-prevention plan, adopt policies that encourage everyone in the company to report suspicious activity. And revise managers' job descriptions to include SOX 806 compliance as one of their responsibilities. At the same time, limit the number of people who receive and document complaints. Keep the sharing of this information on a "need-to-know–only" basis.

But what if you need to fire an employee who's made a whistleblower report, for reasons unrelated to the complaint? Ensure that you have clear and convincing evidence that your action isn't retaliatory. As a practical matter, that means you need plenty of documentation, including a record of unacceptable performance or activities, with dates, and the action taken following each incident. You may also want to discuss the situation with your attorney before terminating the employee.

Under SOX 806, a whistleblower can sue you individually for wrongful retaliation, and criminal penalties can be as high as 10 years in prison. Even if the whistleblower's accusations are ultimately proven false, your company's image is likely to be tarnished by a prolonged dispute.

Start with an ethical culture

If you aren't aware of all the provisions of SOX 806, become familiar with them now. Even more important, take steps to ensure that your company is held to high ethical standards, which includes strong fraud controls, regular audits, and simple and confidential fraud reporting opportunities. ■

Are death bonds a healthy investment?

Inflation and a sluggish economy are helping the death bond, or viatical, market boom. The popularity of these types of investments has, in turn, opened yet another door for criminals.

New twist on revived scheme

Now generally called life settlement-backed securities, viatical investments are purchased from the elderly or terminally ill, who receive up-front payments for their eventual life insurance policy death benefits. Viatical investors are gambling on when the policyholders will die. So these investments carry risks, but the rewards often outweigh them.

Recently, a new twist on an old investment was introduced. Investors may now buy interests in the death benefits of healthy seniors for even greater risk and higher potential returns. Even though these are legal investments, many of the businesses that have sprung up to facilitate them are shady. One of the most notorious, Florida-based Mutual Benefits Corp., bilked approximately 30,000 investors out of close to a billion dollars over nearly a decade.

Another company, American Benefits Services, operating in Texas, collected $117 million from more than 3,000 investors, Financial and Tax Fraud Associates reports. American Benefits forwarded the money to another viatical settlement company, Financial Federated Title & Trust, which spent $111 million on a helicopter, boats, luxury cars, houses and large salaries for its company organizers. The other $6 million went to life insurance policies for investors.

Do your due diligence

Death bonds are legitimate investments when they're offered and administered by reputable companies. If you're considering them, do your due diligence just as you would with any other investment. Find out if the seller and the investment are licensed in your state and obtain a prospectus and other written documents that contain enough information for you to evaluate the offering. If the rewards seem unusually high, ask a financial professional for a second opinion.

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