Forensic Focus

Insights on fraud detection and deterrence

APRIL/MAY 2008

Use a risk assessment to fight fraud before it starts

Who benefits from your energy program?
Con artists exploit conservation efforts

Trust isn't enough
Nonprofit organizations must guard against fraud

"Red flags rule" boosts business security requirements

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

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

Use a risk assessment to fight fraud before it starts

If you discover an employee is embezzling from your company, you're likely to act quickly to learn the extent of the fraud and how it occurred. But if you're like most business owners and executives, you may not be as quick to search for weaknesses *before* a fraudster gets a chance to exploit them.

Under the Sarbanes-Oxley Act (SOX), publicly traded companies must conduct fraud risk assessments, though SOX and federal regulators have offered little guidance on how to do that. Privately held businesses are under no such legal obligation, but it's in their best interests to assess their fraud vulnerability with the assistance of a forensic accountant. In fact, a thorough risk assessment should be the core of every company's antifraud program.

Don't skimp

But where in the company do you start looking for vulnerabilities? Accounts payable? Purchasing? Information technology? A comprehensive fraud risk assessment should include all those areas, and more; you really can't afford to skimp. If you close a door in only one department, those bent on fraud will find openings elsewhere.

Look at your internal controls in the same way a dishonest employee would assess them — as opportunities with relatively little risk of exposure. There are four major ways employees might exploit holes in your system:

1. Fraudulent financial reporting, such as improper revenue recognition and overstatement of assets,

2. Misappropriation of assets, including embezzlement or theft,

3. Improper expenditures, such as bribes, and

4. Fraudulently obtained revenue and assets, including tax fraud.

Some schemes, such as payroll fraud or kickbacks, may involve external people in addition to internal ones. And bear in mind that fraud may be limited or widespread — affecting everything from individual accounts to entitywide processes. Your controls should address all levels, as well as all types, of fraud.

Ask questions

Start assessing your risk by interviewing key executives and managers. They'll provide you with a first glimpse of potential risk areas. Perhaps more important, these conversations will help you judge whether company leaders are setting the ethical "tone at the top" that's integral to fraud prevention.

Next, identify the number and names of employees who handle or review accounting functions. How many, for example, reconcile bank statements or are authorized to make bank deposits? And are accounting employees required to take at least one week of vacation each year? The fewer employees involved in financial functions, and the less vacation time they take, the greater your risk for fraud.

Spreading accounting and banking duties across multiple employees — or shouldering some of the review processes yourself — provides segregation and oversight that are essential to deterring fraud.

Regularly review organizational charts to ensure constant segregation of duties.

Other issues to consider include:

Key performance indicators. Entitywide fraud can show up in the performance of sales goals or inventory management. It's important to take fraud risk into account when establishing key performance indicators, as well as to review them regularly with an eye to the unexpected.

Fraud-risk management budget. Compliance training, internal controls monitoring and ongoing risk reviews take time and money. The extent and cost of such activities will vary among companies, but they should be included in your business's budget.

Strategy updates. Risks change, and you need to change with them. Evaluate your risk management practices regularly — annually, if possible — to identify and address any new weaknesses.

Focus where it matters

When analyzing your findings, remember that your company's processes, procedures, programs and policies make you unique. Your results aren't likely to be the same as those of other companies — even in the same industry. That shouldn't keep you from benchmarking against best practices, but you should concentrate on your own areas of greatest risk. A manufacturer that regularly purchases parts inventory may have more risk of procurement fraud, for example, than a small publishing firm that buys only office supplies.

The fewer employees involved in financial functions, and the less vacation time they take, the greater your risk for fraud.

Next, consider less-critical areas. Typically, you should have one key control for each risk. If payment authorization is a risk area, for example, you could require multiple approvals for expenditures over a certain amount. Alternatively, if the risk is great enough, you may decide to alter a business process to remove the risk rather than attempting to control it. If you determine that a manual check-writing control is inadequate, for example, you might choose to automate check payments rather than add more controls to the manual system.

Don't let fraud get a foot in the door

If your human resources department doesn't already, it should make background checks a routine part of your company's hiring processes. People in heavy debt or involved in litigation, for example, may be willing to do whatever it takes to get the money they need. And job candidates with criminal records — or even a history of traffic tickets — may be less likely to follow your company's ethical guidelines. They may also be adept at breaking the rules without getting caught.

Be sure to assess all the risks associated with a process, too. For example, you've probably surrounded your IT system with firewalls, intrusion detection alarms, virus protection and other guards against outside invaders. But are you guarding against intrusion from *inside* the fence? Keep activity logs for company data servers, as well as itemized logs of calls made from office phones and corporate cell phones. Require employees to password-protect sensitive files, and monitor to make sure that passwords are in place and that they aren't being written down or shared freely.

Finally, if you don't have a fraud hotline, consider establishing one. Time and again, research has found that tips from employees are one of the most effective ways to expose fraud. To be successful, though, hotlines must be convenient and confidential. You may also want to establish a hotline for customers and vendors, or give them access to the employee tip hotline.

Cultural commitment

Regardless of what your fraud risk assessment reveals, you need a strong antifraud policy — which you can create with a forensic accountant's assistance — and you must communicate it regularly and emphatically. One of the best deterrents to fraud is a company culture in which fraud is absolutely not tolerated. If you and your senior management are visibly committed to honesty, integrity, fairness and equity in all your operations, your employees will follow suit. ■

Who benefits from your energy program?

Con artists exploit conservation efforts

Oil prices were recently at record highs, global warming dominates the headlines, and companies are under pressure to reduce greenhouse gas emissions and conserve energy. This heightened awareness ultimately may benefit the environment — but it's already proving profitable for opportunistic con artists.

Pumping up

Alternative energy scams come in several forms, but the most common are related to investments. These days, many investors are legitimately interested in alternative energy stocks, and fraudsters are eager to take advantage of this demand.

Energy-related stock fraud typically involves pump-and-dump schemes. The fraudsters create demand for a small, unknown company's stock with exorbitant price promises, misrepresentations and hyperbole. Offers and claims such as "Everyone should have an alternative energy stock in their portfolio. This is the one!" are spread via fax, e-mail and even cell phone text messages. When their marketing efforts push the price of the stock up, the scam artists sell off their shares, and the stock deflates.

These pitches are aimed largely at consumers, but they can affect business investment decisions as well. In one recent case, two companies were found guilty of trading nonexistent energy futures on a nonexistent exchange through a fraudulent broker.

Partnership foibles

Other investment-related scams involve oil and gas limited partnerships. These investments — which typically become available when oil prices rise — can be legitimate and profitable. They also are highly speculative and extremely risky.

In a fraudulent deal, the limited partnership might be in one state and the operations in another. To reduce the risk of investors dropping by a

nonexistent site, the scammers offer the investment "opportunity" to businesses and individuals outside either state. What happens after that varies by scheme, but in one version, the company claims it has hit a dry hole and then asks investors for more money to cover the costs of full production.

In another scenario, a company drills several holes for oil and hits on one. That becomes the one it owns outright, while the dry holes are financed through investors.

No credit

Some companies eager to "go green" attempt to offset their energy use by buying carbon credits from companies that don't use as much energy as they're allowed. The credits are intended to cancel out larger energy consumers' contribution to global warming. But according to a *Financial Times* investigation published in April 2007, companies around the world often buy worthless credits. Brokers may provide services of no value, and a shortage of verification procedures makes it difficult to determine the true value of carbon credits.

Other questionable practices involve companies that ask customers to pay additional fees to help eliminate greenhouse gases in their manufacturing plants. The

equipment required to reduce the gases is relatively cheap, so the companies are pocketing potentially sizable sums in the name of environmental responsibility. Or they may invest in enhanced oil recovery efforts that pump carbon dioxide into depleted oil wells to extract any remaining oil. With the price of oil high, recovery is already profitable, and operators are just making extra money selling carbon credits for burying the carbon.

While neither of these practices may actually be illegal, they aren't truly forthright, either. And they provide further evidence that joining the energy conservation movement requires conviction *and* caution.

False claims

Scammers have also found a way to capitalize on fuel-saving and emissions-reducing devices for vehicles. One such fraud involved FuelMax and SuperFuelMax products, which marketers and resellers claimed would increase gas mileage 27% and reduce fuel consumption and emissions.

As attractive as these claims might have sounded to companies that devote a big chunk of their budgets to transportation, the Federal Trade Commission found that the products provided none of their advertised benefits. The manufacturer, International Research & Development Corp. of Nevada, was ordered to pay $4.2 million for redress.

The time is now

Alternative energy's time appears to have come — but with a hefty caveat of "let the buyer beware." Whenever there's an opportunity to make money, criminals are prepared to exploit it. So before putting your money in an energy-related investment or energy-saving program, ask a forensic accountant to review it. ■

Trust isn't enough

Nonprofit organizations must guard against fraud

Janet was 50 miles from home when a teenager drove his car into hers. She wasn't hurt, but her car was badly damaged and undrivable. Perhaps worse, her credit card was near its limit and wouldn't cover towing and a rental car.

But Janet worked for a nonprofit organization, and she had that organization's credit card with her to buy supplies for an upcoming fundraiser. She reasoned that, because this was an "emergency," it would be OK to use the card for personal purposes.

That kind of reasoning is what makes fraud against nonprofit organizations possible — even common. Because their cultures are oriented toward helping others, nonprofits often find it impossible to imagine that anyone working for them would steal. The reality is, people who defraud nonprofit organizations typically are liked and trusted employees and volunteers who otherwise appear committed to the cause.

Cultural vulnerability

When no one mentioned her emergency credit card expenditures, the fictitious Janet started taking advantage of the card for other, relatively small personal expenses. By the time someone at the organization finally noticed, she had racked up charges totaling nearly $10,000.

Nonprofits rely heavily on volunteers, and they aren't known for paying high salaries to employees. But organizations that allow workers to feel like martyrs unwittingly promote fraud. Fraud perpetrators often rationalize that they deserve more than they're getting, so they help themselves.

Potential fraudsters also typically think that the consequences of getting caught are minimal. Unfortunately, this belief is valid in many charitable organizations. Nonprofits often fail to prosecute fraud because they fear it may damage their reputations as

responsible stewards of donors' money. Instead, they quietly fire the offender and suffer the losses.

Opportunity knocks

Far too many nonprofits don't have in place the basic internal controls that discourage fraud. They often, for example, fail to conduct background checks on volunteers responsible for fundraising and canvassing. And not all organizations require volunteers to provide receipts for cash donations. Thus, anyone willing to volunteer time could easily skim donations for personal use.

Billing schemes are potentially even more damaging. Most involve fictitious vendors or collusion with actual vendors willing to submit false or inflated invoices. The employee or volunteer may approve the invoices or write checks to pay them — or both.

Without a system of checks and balances, anyone can write checks for personal purposes with little fear of exposure. Similarly, if oversight is lax, fraudulent employees may authorize "overpayment" for goods and services for months before being caught.

Oversight needed

Nonprofit administrators and boards of directors can curb fraud. But they must first acknowledge that fraud can occur in their organization and that it's their duty to prevent it. The first step is to establish a culture of honesty that begins in the boardroom and is relayed directly through the executive offices, down the chain of command. Antifraud policies should be in writing and posted where they are visible to everyone.

Additionally, board members should insist on, at minimum, fraud controls in the following areas:

System access. Make sure employees have access only to the information and programs *required* for their job responsibilities, and password protect any sensitive information.

Cash counts. If a volunteer reports the sale of 100 event tickets, make sure he or she turns in a corresponding amount of cash — and the correct number of unsold tickets. Also compare cash receipts logs to the cash receipts ledger entry and actual bank deposit.

Vendor addresses. Periodically compare vendor addresses to those of other vendors and of employees and volunteers. Duplicates should raise suspicions.

Getting boards on board

Nonprofit boards typically are made up of volunteers whose major qualification is that they believe in the organization's mission. They usually have other commitments — such as paying jobs — and sometimes boast only limited financial experience.

Usually, boards rely on executive directors or accountants to monitor the organization's financial operations. And because an annual audit is supposed to ensure that year end financial statements are accurate, board members may feel they've performed their fiduciary duties by reviewing the audit results.

Those members are closer to being right, thanks to new audit requirements. Auditors now must look at processes and internal controls, as well as checking the accuracy of an organization's bookkeeping. They also are required to assess the training and expertise of the organization's staff, making sure that those who enter transactions into the system understand the processes governing the transactions.

Board members need to realize, however, that an annual audit based on sampling isn't a foolproof fraud-detection tool. They also need to help their auditors design effective internal controls — and then be sure the controls are enforced between audits.

Bank statements. Have someone other than the individual writing checks — preferably a board member — receive unopened monthly bank statements and review them.

Finally, if you require dual signatures on large checks, don't rely on your bank to notice that one is missing. Require approvals and oversight to ensure the rules regarding disbursements are being followed.

Keep current

Your antifraud program is only as strong as it is current. Review internal controls periodically for effectiveness, and make changes to address any weaknesses or new challenges. Also, consider buying an employee dishonesty insurance policy, which can help you recover losses should you be defrauded. ■

"Red flags rule" boosts business security requirements

Most business owners want to do their part to help stamp out identity theft. But the federal "red flags rule" issued Nov. 9, 2007, may require them to shoulder more of the load.

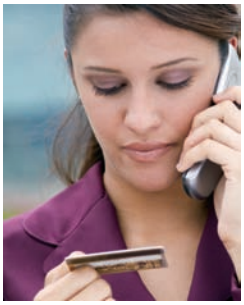
New rules

By Nov. 1, 2008, all financial institutions and creditors must have programs in place that enable them to detect and prevent identity theft and to identify certain patterns and practices that suggest fraud. Businesses that collect or use customer loan or credit information — such as auto dealers or retailers — are considered creditors and, thus, must comply with the rule.

The new rule is an expansion of the Fair and Accurate Credit Transactions Act of 2003. It's intended to curb fraud in the opening of covered accounts — those that are established primarily for personal, family or household purposes and are reasonably vulnerable to identity theft.

Patterns and practices

Some requirements, such as ensuring that a customer's driver's license photo matches his or her face, are easy enough to implement. Others, including reporting patterns or practices that might indicate potential identity theft, take greater effort and may require expert assistance.



Suspicious activities are likely to vary from one business to the next but could include customer address discrepancies, an unusual number of newly opened credit accounts or incomplete personal information on a credit application. To report them, train employees to recognize unusual activities and take appropriate steps to validate and mitigate risk.

A forensic accountant can help you develop a written program that includes policies and procedures to define and detect red flags when they arise and respond appropriately to them. Programs must be updated regularly to reflect changes in risks. Additionally, you must put systems in place to verify change-of-address requests and to notify the account holder if an address provided substantially differs from the one you have on file for the holder.

Taking responsibility

In the past, businesses have been able to rely on credit reporting agencies or parent corporations (such as automobile finance companies) to conduct such checks. As of Nov. 1, however, your business may have to assume additional responsibility. ■

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