

fraud alert

june/july 2007

Building a fraud risk management program that works

**Ethical sales isn't
an oxymoron**

**Dream candidate
or nightmare?**

**Use reference checks to
improve your hiring success**

**Don't get fooled by phony
health insurance plans**

**Fraud to watch for:
Caller ID spoofing**



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

Building a fraud risk management program that works

Corporate fraud remains a significant threat to businesses, despite legislative efforts to address it. Nevertheless, too many businesses have yet to adopt comprehensive, integrated fraud risk management programs. If you've put off taking this important step toward protecting your company, now is the time to act.

Know yourself

To be successful, your fraud risk management program should encompass all levels of your organization, starting at the top. It should meet three primary objectives: prevention, detection and response.

The first significant challenge is understanding where you're at risk for fraud. Be specific and realistic. Your vulnerabilities aren't necessarily the same as those of similar-size businesses or even of your close competitors. You may, for example, already segregate duties in your purchasing department, while your competition may have stopped with password protections.

You need to examine your risk objectively, as well. The question isn't whether your long-time bookkeeper *would* embezzle funds; the question is whether he or she *could*. In assessing your risks, consider both internal and external opportunities for malfeasance and how employees at any level of seniority could work alone or in concert to exploit them.



Once you've performed a thorough review of your company's existing practices, consider the overall costs of your risk, including the consequences and long-term impact of letting it go unaddressed. Recognize that risk management is more than buying insurance; risk management is working to ensure that you don't need insurance because you're taking steps to close gaps that fraudsters could exploit.

Put it in writing

Next, turn your attention to preventive strategies. If you don't have a written code of ethics and business conduct, now is the time to develop both. Fraud prevention begins at the top, with a clearly communicated commitment on the part of management. It isn't enough that you have a code of ethics; you must be seen following it.

Then look at your internal controls. Did you consider fraud prevention when you designed them? If not, re-evaluate them with an eye to closing possible loopholes. Policies to consider implementing include:

- Segregating financial and accounting duties,
- Duplicating sensitive tasks such as by double-signing checks over certain amounts,
- Requiring annual vacations for employees,
- Reconciling all bank accounts,
- Using passwords and IDs on computer files,
- Restricting unauthorized access to offices and computers,
- Training supervisors and managers to spot fraud, and
- Performing internal and external audits that include scrutiny of fraud prevention measures.

It's important, too, that you don't allow the employees who create fraud policies to assess and manage them. If, for instance, your IT staff devises its own security measures, someone outside the

Follow-through is essential

Many companies, fearing harm to their reputation, are reluctant to prosecute employees caught with their hands in the cookie jar. But you need to get over that fear. When you design a fraud risk management program, don't skimp on planning a thorough and effective response to fraud incidents.

When fraud occurs, your first reaction may be to correct the flaws that allowed it to occur and, simultaneously, remedy whatever harm was done. But you'll also need to demonstrate to both internal and external stakeholders that you take fraud seriously. A well-designed disciplinary process that's implemented immediately and impartially — regardless of rank or tenure — can send that message.

You can implement a series of progressive sanctions, from verbal warnings to termination — depending on the seriousness of the offense. In deciding what's appropriate, keep in mind that managers also should bear some responsibility if they haven't trained their subordinates properly or have pressured them to achieve unrealistic goals.

department should determine whether the measures are appropriate and adequate and monitor whether they're being followed.

Set priorities

Once you've determined your areas of risk and ways to address them, you may discover that you can't do everything at once. If so, set some priorities so you can allocate resources most effectively.

Understand that not all risk is created equal. Some risk has the potential to cause damage that will ripple


throughout the company but, viewed objectively, is highly unlikely to occur. Fraudulent financial reporting, for example, can topple a company, but heightened attention among auditors and the public, combined with Sarbanes-Oxley-driven internal changes, make it more difficult to perpetrate today.

Other potential problems may do less damage, but there's a much better chance that they'll happen. An over-worked bookkeeper with a heavy mortgage could, for example, exploit operational loopholes to embezzle money fairly easily. In deciding how best to allocate your fraud prevention resources, assess the probability of different risks, rather than simply their size.

You also should set up a continuous monitoring system that will allow you to track and adjust controls as changing circumstances require.

Fraud risk management isn't a one-off: You must constantly evaluate your existing controls, comparing them with legal, regulatory and best practice standards.

Look over your own shoulder

Fraud risk management can be time-consuming and complicated to design and implement, but it's nothing compared to the stress and potential financial losses that a fraud scheme can create. It's worth the initial headaches to have the peace of mind that a good fraud prevention program can deliver. 

Ethical sales isn't an oxymoron

You know you're operating a reputable business, but is that the impression your sales force is leaving with potential customers? Or is your sales team willing to say whatever it takes to seal the deal? In today's cutthroat business climate it's easy to lose sight of what constitutes an ethical sales program. To preserve your company's good name, don't overlook your sales force when building an ethical business culture.

Walk the talk

Culture starts at the top. If you clearly demonstrate, through both words and behavior, your commitment to honesty and integrity, your sales team will get the message — and so will your customers.

Next, try to anticipate the challenges your sales force may face as they attempt to meet sales goals.

The temptation to sell more than your company can deliver, for example — or to recommend a product they know isn't the best solution for a customer's problem — may be strong. Those and similar sales strategies may land the account, but they do nothing to build the trust and credibility your business needs to keep that account over the long haul.

It's also important that your company and salespeople don't try to slip through loopholes when the situation requires taking responsibility. Some insurance companies that wrote coverage on homes and businesses damaged during Hurricane Katrina, for example, have lost significant goodwill. When they were asked to pay out on those policies, they quibbled over whether the damage was due to wind (which was covered) or water (which was not). The ensuing legal battles and negative publicity, which continue nearly two years after the storm, have done nothing to raise consumer confidence in insurance.

Make things clear

When your salespeople make a sale, require them to be clear about what that sale includes and what it doesn't. Reiterate that their job isn't simply to make sales, but to build lasting customer relationships. To do that, they must always keep the customers' best interests in mind. To make sure the message gets heard, consider using measures for customer satisfaction and repeat business, in addition to sales revenue quotas, to determine sales rewards.


That may mean acknowledging, for example, that one of your products won't do everything the customer needs it to do. If a customer asks about a feature your product doesn't have, your sales reps shouldn't try to imply that it does.



Instead, they should work with the customer to determine whether the desired feature is really necessary and emphasize your product's other features and benefits. Ultimately, however, they must be honest about your product's limitations.

Your sales force doesn't need to steer a customer to a competitor, but they shouldn't disparage the competition, either. And incentivizing customers to load up on unneeded products during promotions may boost the bottom line, but it won't do much to build trust.

Integrity = success

If you want to help ensure your sales department is operating ethically, emphasize that professional integrity is a big part of your definition of success. This attitude will go further in promoting the health and longevity of your company than sales campaigns that operate at the expense of customers. 

Dream candidate or nightmare?

Use reference checks to improve your hiring success

You've found your dream job candidate: She's bright, personable and experienced, and has all of the required skills. You're tempted to hire her on the spot to get her on the job as soon as possible. But before you make an offer, be sure you check your candidate's references.

Sure, the references she lists probably will have positive things to say, and tracking them down may be time-consuming. It will be time well spent, though, if it helps you avoid a bad hire who damages morale, falls apart in a crisis or even steals. It also could save you from wasting thousands of dollars

and several months getting rid of her and finding a replacement.

Consider your sources

The reference check process should begin as early as the interview stage. When you ask your job candidate about a project that went well, follow up by inquiring about others involved in it. You need to contact the references a candidate provides, but you'll probably get more information from supervisors, peers and subordinates who aren't on the list. These individuals may be able to provide specifics on the extent to which your candidate is responsible for a project's positive outcome and how well he or she works with others.

Before you talk to anyone who isn't on a candidate's list, however, make sure the candidate understands that you'll be looking beyond those names. Ask if there's anyone you can't consult. After all, you don't want your prime candidate to think of you as a sneak.

When you're ready to start calling references, prepare your questions to elicit the most enlightening responses. You want to verify factual information from the resumé, but don't supply the answers as you ask the questions. Ask for dates of employment, for example, rather than asking whether it's true that Sam Smith worked at the company from 1998 to 2006.

From there, move to questions that will generate less structured comments. If you remain conversational rather than interrogatory, the reference will likely feel comfortable opening up. Ask, for example, how well the person knows the candidate and how closely they worked together. Then ask about specific tasks or projects the candidate described during his or her interview.

Yakety yak

Other questions you may want to ask during reference-check conversations include:


- How well does the candidate follow through on projects?
- What is his or her management style (if the candidate is in line for a management position)?
- Would the former employer hire the candidate again?
- What advice would they give the candidate's next employer?

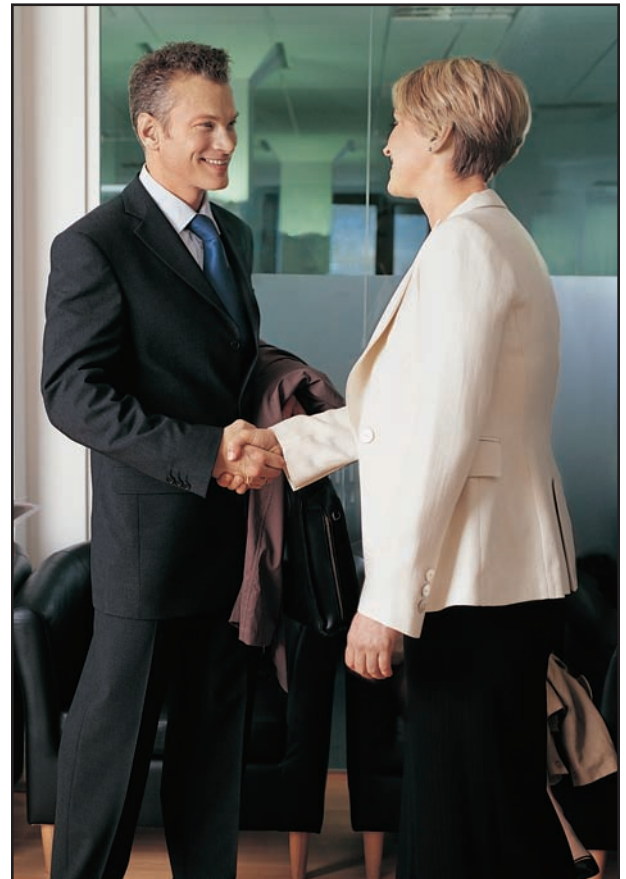
- What would the candidate's critics say about him or her?
- If the candidate is seeking a position that involves handling large sums of money, are they aware of any reason he or she shouldn't be considered for the position?

Pay attention to how the reference phrases answers, being sensitive to evasiveness, hesitancy and equivocation. Be wary, for example, if a question about whether the reference has ever known the candidate to pilfer office supplies elicits a response such as "Well, I don't know for a fact ... but doesn't everyone?" If someone waffles, it may, in fact, be a sign that the reference knows of more egregious offenses.

At the same time, keep in mind that references filter their views through their own lenses. They may have personal agendas that prevent them from giving you a fully objective or accurate view of the candidate.

Wealth of information

Reference checks can be a waste of time if you don't approach them correctly. Do them right, however, and you may uncover a wealth of information that can keep your dream candidate from becoming a nightmare of an employee. 



Don't get fooled by phony health insurance plans

Businesses looking for ways to combat the skyrocketing cost of health insurance can find themselves financially responsible for a lot more than health insurance premiums if they fall prey to con artists selling phony coverage. Insurance scammers take advantage of the fact that companies are under pressure to keep costs in line by selling coverage at a deep discount. Knowing how to spot this type of fraud may be essential to the continuing financial health of your business.

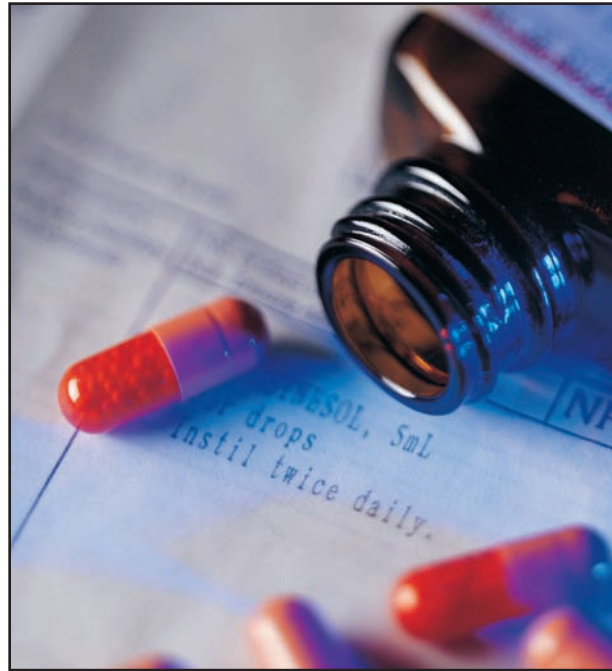
Too good to be true

Typically, health insurance fraudsters offer group coverage at extremely low rates — as much as 50% below usual premiums. And the plans come with few or no qualifying restrictions, such as coverage delays for existing conditions. Agents may ask only that you join a “union” or “association” and write them a check for the premiums. They won't have a state license to sell insurance, but they'll claim they don't need one because the plans they're selling are regulated under federal ERISA laws.

Everything may seem legitimate until one of your employees submits a claim. Sometimes phony programs use a small percentage of the premiums they're collecting to pay a few inexpensive claims. But in most cases, business owners and their employees are left with nonexistent coverage and mounting, unpaid health care bills.

If the agent is in a hurry to sign you up, or doesn't have solid answers to direct questions, keep looking.

When the coverage doesn't materialize for major procedures such as kidney transplants or chemotherapy, the out-of-pocket expenses can force individuals and businesses into bankruptcy. Worse,



lack of coverage may cause employees to delay needed care — with potentially dire results.

Signs of distress

When shopping for group health insurance, look for signals that someone is trying to take you for a ride. These include:

- Coverage costs that are 25% or more below normal rates but include a large provider network and generous benefits,
- Immediate acceptance of participants with serious pre-existing conditions,
- Few or no underwriting guidelines,
- An agent who isn't licensed in your state,
- An agent who can't adequately answer your questions or is reluctant to provide specific information,
- An unfamiliar company name, or
- A requirement that you join an “association” that doesn't provide information about its membership or have bylaws.

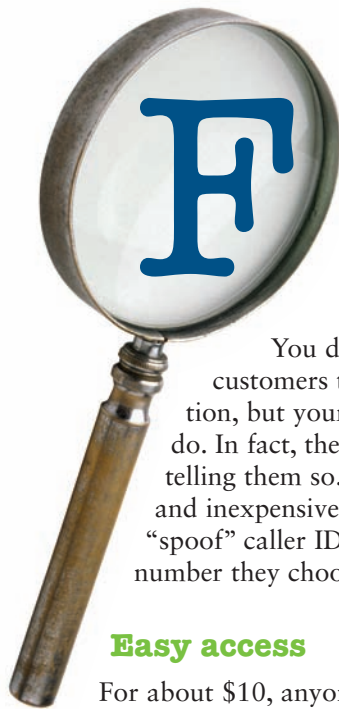
As is true with many types of fraud, if the deal sounds too good to be true, you need to be wary. Scrutinize the company's name — it may just be a variation on a legitimate insurer's name. The bogus United Employers Voluntary Employee Beneficiary Association, for example, could be misconstrued as an arm of the reputable UnitedHealthcare.

Check with your state insurance department to see if the company is licensed or has been the subject of

complaints. And if the agent is in a hurry to sign you up, or doesn't have solid answers to direct questions, keep looking.

Money for nothing

Every company feels squeezed by health care costs these days. But while affordable health coverage can be difficult to find, any legitimate policy — no matter how expensive — is better than paying for nothing. ¶



raud to watch for: Caller ID spoofing

You don't call your clients and customers to ask for personal information, but your customers may think you do. In fact, their caller ID systems may be telling them so. Thanks to readily available and inexpensive software, scam artists can "spoof" caller ID numbers to make any number they choose appear on the other end.

Easy access

For about \$10, anyone can buy a 60-minute calling card on the Web. Users call a toll-free number, enter a personal identification number, the caller ID number they'd like to display and the number they'd like to call. In some cases, they also can select whether the voice the call recipient hears is male or female.

Many spoofers pose as representatives of banks, churches or other respectable institutions. They may say they're owed money or that there's a problem with an account — all in an attempt to obtain Social Security or bank account numbers. Alternatively, posing as customers, technicians or even regulatory officials, they may call businesses to obtain confidential business information.

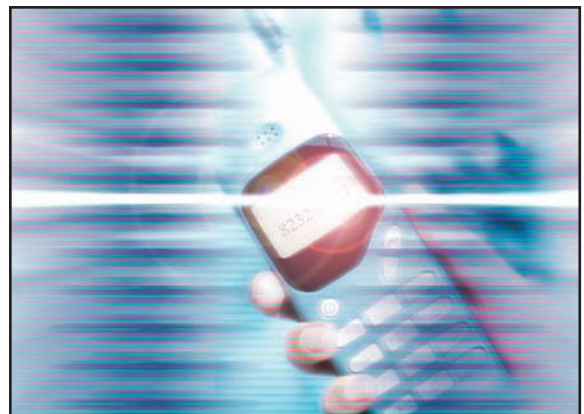
Old dog, new tricks

Caller ID spoofing is to telephones what "phishing" was to e-mail several years ago. As phishing gained notoriety, people became warier and the scheme became less attractive to fraudsters. As

easy-to-use calling systems have become available in the last couple of years, scam artists have turned to spoofing.

The good news is that phone companies can track calls to their sources regardless of what caller ID says (although it's a long process that may involve several phone companies). The not-so-good news is that caller ID spoofing appears to be legal. The Truth in Caller ID Act of 2007 pending in the U.S. House of Representatives, however, would change that.

In the meantime, people who rely on caller ID to identify callers — both at home and at work — should remember the adage: Trust, but verify. Knowing who is or isn't really on the other end of a telephone line can save hard feelings, as well as cold, hard cash.



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

