McGOVERN & GREENE LLP
Certified Public Accountants & Consultants

fraud alert

august/september 2007

Shell games
Are you being played?

Dial "F" for fraud
Encouraging employees to use anonymous hotlines

Know-your-customer programs
Not just for banks

Fraud prevention is a cost small businesses can't forgo

Fraud to watch for:
Affinity fraud

McGOVERN & GREENE LLP
Certified Public Accountants & Consultants

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

Shell games

Are you being played?

For a nominal fee, prospective business owners can get a "doing business as" (DBA) certificate from any county clerk's office under the name of their choosing. For many entrepreneurs, DBAs are a cost-effective way to open a small business. And for fraudsters, DBAs can be a cost-effective way to create shell companies they can use to steal from their employers.

Shell companies — businesses with no assets of their own — may serve legitimate business purposes, such as holding another company's assets. But they also may be used to perpetrate fraud.

Stealing on the cheap

Recent media coverage of shell companies has focused on large-scale fraudulent undertakings, including stock market manipulation, terrorist funding, money laundering and tax evasion. The problem is so great, in fact, that both the Securities and Exchange Commission and the IRS recently have made changes to tighten regulatory loopholes that will more easily expose individuals who are hiding income.

For most businesses, however, the larger threat of shell companies may be that unscrupulous employees will use them to perpetrate billing fraud — a scheme that generates a median loss of $130,000, according to the Association of Certified Fraud Examiners' 2006 *Report to the Nation*.

Money for nothing

Billing fraud that uses shell companies can take two forms. In one, dishonest employees set up a shell company to send out — and collect on — fictitious bills. Of course, perpetrators don't even have to send the bills for nonexistent goods and services to the company for which they work. But it's easier, and can help them evade detection, if they do.

Consider, for example, an accounting employee who knows that her company rarely scrutinizes invoices for less than $2,500. She can get a DBA certificate for a fictitious business, using a post office box or accomplice's address, and open a business account at a local bank. Voila! She's ready to start billing her employer for services that cost less than $2,500 per invoice.

The second type of shell-company-based billing fraud is a pass-through scheme. Again, an employee sets up a fake company. This time, however, he uses it to buy goods or services his employer requires and then sells them to the employer at a marked-up price. Because the employee's shell company has no overhead or expenses, he pockets the proceeds.

Following the paper trail

Shell company schemes can go undetected for a long time, particularly if the fraudsters are savvy enough to attempt to cover their tracks — and if they don't get too greedy. Most perpetrators, however, leave a paper trail flagged with warning signs that are visible to informed eyes. These include invoices that:

- Poorly define their products or services,
- Have a company address that matches an employee's home address,
- Use a post office box as their return address,
- Have a company name that matches an employee's initials,
- Arrive more than once a month, and
- Show an increased number of purchases over time.

None of these in isolation is proof of fraud, but any of them warrants a closer look. Taking the time to scrutinize a company's operating practices also is wise.

A shell company scam perpetrated by an accounting employee, for example, works only if the employee can pay the invoices or get the shell company authorized as a legitimate vendor. A quick credit check on a new vendor will reveal whether it has an operating history, and a glance at a telephone directory will show whether it's listed outside of your company's records.

System of checks

It's very easy to start a business, but that shouldn't give fraudsters a free hand to rip off or even destroy yours. Familiarize yourself with the signs of shell company abuse and put in place a system so that you'll catch billing fraud before it begins.

Shell company ownership murky, GAO report notes

The Government Accountability Office (GAO) reported last year that states don't routinely collect ownership information on applications for new, non-publicly traded companies. In addition, the GAO noted in its report to the Senate Permanent Subcommittee on Investigations that third-party agents may submit papers without collecting or verifying ownership information.

As a result, investigations of suspicious shell companies sometimes are stymied because investigators can't identify their owners. For example, Immigration and Customs Enforcement couldn't prosecute one case involving a Nevada-based firm that received more than 3,700 suspicious wire transfers totaling $81 million over two years, simply because the agency couldn't discover who owned it.

On the other hand, states say collecting more ownership information could increase costs, raise privacy concerns and mean loss of revenue if owners opted to form shell companies in other jurisdictions. The record made no recommendations, but noted that, if additional ownership disclosure were to be required, conflicting concerns should be balanced and that any such requirements would need to be applied uniformly across all jurisdictions.

Dial "F" for fraud

Encouraging employees to use anonymous hotlines

Anonymous hotlines have been demonstrated to be cost-effective and successful mechanisms for detecting occupational fraud, but you can't just build them and expect tips to come. Like any other business process, hotlines must be properly established and maintained if they are to provide expected returns.

Don't scare them off

The Association of Certified Fraud Examiners has found that fraud is most often revealed through tips, and that tips generally come from employees who know or suspect fraud is being committed. But while the existence of a hotline can be enough to prompt second thoughts in employees tempted to commit fraud, it isn't enough to encourage reports of actual activities.

To do that, a hotline must be convenient, confidential and anonymous for tipsters. Potential whistleblowers should feel secure enough to overcome their reservations about "ratting" on co-workers and be able to control their nerves long enough to dial the phone. If they can't connect the first time, they might not try again.

Make it easy

First and foremost, your fraud hotline must be available 24 hours a day, seven days a week. Few employees will risk making reports during working hours — regardless of how unlikely they are to be overheard. They're much more likely to call during the evening from their homes or mobile phones.

Second, the hotline should be more than a voicemail system that forwards calls to another department. While it's

true that some company officials ultimately will be involved in investigating hotline tips, employees are more likely to speak freely to a third party or a designated individual within the company than to an anonymous department phone.

From your point of view, a line that's monitored around the clock is likely to be more valuable, as voicemail messages may not contain the information you need to mount an investigation. But if that's not possible, don't be tempted to use caller ID or other identifying features that would allow you to gather additional data from the caller. The perception that calls aren't anonymous will discourage reports.

Instead, educate employees about what information they must provide when reporting suspected wrongdoing and reiterate that all calls will be kept confidential. Additionally, emphasize that callers will be protected against possible retaliation. You might communicate this information in your company newsletter or on your intranet, or by posting it in employee breakrooms.

Show results

Be sure you can back up your words with actions. Demonstrate that you take anonymous tips seriously by tracking complaints, investigating them thoroughly and reporting their dispositions not just to internal audit and fraud-prevention personnel, but also to employees.

Without revealing details, let employees know how many reports you receive each month or quarter and how many disciplinary or legal actions resulted from them. If you also report the number of tips that proved to be unfounded, and why, you may be able to discourage frivolous attempts to discredit innocent co-workers.

Finally, remember that a hotline is just one factor in your overall fraud prevention efforts. You also need a company culture that actively discourages fraud from the top down, as well as a strong set of internal controls to make fraud difficult to perpetrate in the first place.

Plan for the best

You're responsible for setting the ethical tone of your company, which includes providing a mechanism for employees to report suspected illegal behavior. A fraud hotline can be valuable in this regard, but you must be sure to build it wisely or the tips won't come.

Know-your-customer programs

Not just for banks

The federal government has enlisted banks and other federally regulated businesses to aid in their fight against money laundering, terrorist financing and identity theft. Under the Bank Secrecy Act, these businesses are required to implement know-your-customer (KYC) programs to help ensure their customers are who they say they are. Even when they're not required, KYC measures can be useful to other types of businesses.

Verification essential

Typically, KYC begins with verifying customers' names and addresses and checking them against federally maintained lists of known fraudsters, terrorists or money launderers. In addition, financial institutions are required to monitor transaction trends and high-risk accounts to determine whether certain transactions merit filing a suspicious activity report with the Financial Crimes Enforcement Network (FinCEN). High-balance accounts with erratic transfers, for example, could be used for money laundering.

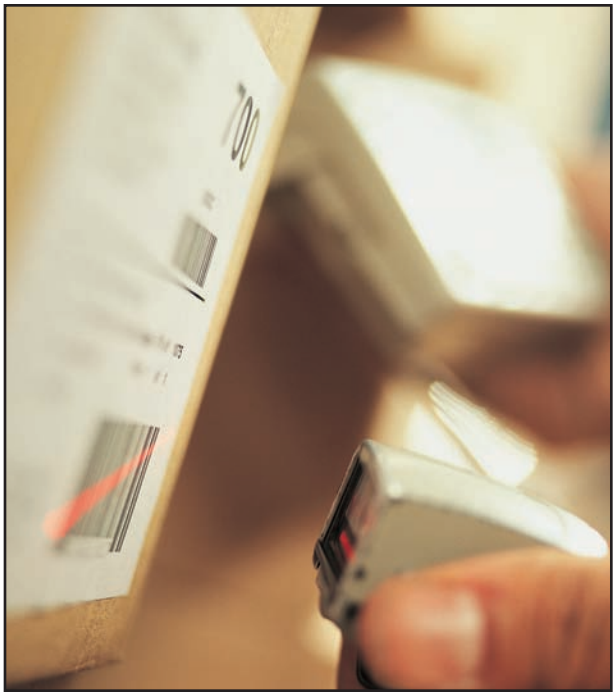
Financial institutions aren't the only businesses with KYC responsibilities. Companies that export products also must be careful not to sell to an individual or

entity on any of five lists maintained by the federal government, including:

- *Denied Persons*, or those who have been denied export privileges,
- *Unverified*, made up of parties involved in previous transactions for which the end use couldn't be verified,
- *Entity*, or those subject to specific Department of Commerce export restrictions,
- *Specially Designated Nationals*, composed of parties with whom exporters may not do business, and
- *Debarred*, a list of individuals and entities the State Department has barred from participating in export transactions.

Exporters also are expected to review all information they receive about customers to ensure that nothing should have alerted them to the possibility a violation could occur. For example, if a customer is willing to pay cash for an expensive item that usually would call for financing, has no business background or lists a freight forwarding firm as the product's final destination, exporters are expected to be wary.

Businesses that fail to be vigilant can face significant penalties. In one recent case, Structural Dynamics Research Corporation (SDRC) was fined nearly $60,000 by the Department of Commerce for selling software to customers in India and China that were on the Entity List and thus subject to export licensing requirements. Although neither the software nor other customers in those countries required export licenses, KYC procedures should have alerted SDRC that they were engaged in risky transactions.



Understanding who your customers are can help prevent you from falling victim to phoenix companies that profit from bankruptcy.

Not your job?

What if you aren't a financial institution and don't sell your products overseas — does KYC affect you? Not directly, but you may want to adopt some of its philosophies anyway. Understanding who your customers are — including performing credit checks — can help prevent you from falling victim to phoenix companies that profit from bankruptcy at the expense of their creditors or to false billing schemes.

What's more, if you create a comprehensive history of each customer's credit limits and transactions, you can identify your top customers. Doing so may not expose fraud or money laundering, but it will help you assess how vulnerable you are should you lose one or a few of your biggest customers.

Also, analyze your customers' purchasing behavior to identify cross-selling and up-selling opportunities — along with any irregularities that could indicate possible nefarious activity. If a customer with a long record of annual purchases suddenly begins placing monthly orders, for example, you should delve deeper. The change may signal nothing more than your customer landing a large new account, but it also could be a sign that someone in your company is cooking the books.

Commonsense approach

KYC is a federal requirement for many financial and export companies. But even if you aren't in those lines of work, knowing who your customers are makes good business sense.

Fraud prevention is a cost small businesses can't forgo

Small business owners may know that they're vulnerable to fraud but not have the staffing or financial resources to implement a fraud-prevention program. Even small businesses with limited resources, however, can take steps to prevent falling victim to fraud. This starts with recognizing that even the most trusted, long-term employee might resort to fraud under the right circumstances.

Get some help

Private businesses aren't required to have annual audits, but you can still work with your accountant to determine where you might be at risk. CPAs can train you to recognize the warning signs and help you reduce opportunities for fraud by, for example, segregating duties in your accounting department.

Periodically request your CPA to review your receipts and disbursements with an eye toward uncovering irregularities. And if you have inventory that could tempt thieves, ask your accountant to verify inventory counts and observe inventory procedures for potential loopholes.

Respect and recognize your employees' contributions to your business, and enlist them in your fraud prevention efforts.

Take action of your own

Of course, you can't rely on your CPA or other advisors for all of your fraud prevention. One area where many small businesses fall short is in conducting background checks on potential employees. At the very least, check all work references. But you also might consider running criminal background checks and requiring drug screenings. Workers with a history of occupational theft often seek jobs with small businesses because they know pre-employment screening likely will be minimal.

Even if you don't have a large enough staff to implement strict segregation of duties, you can still establish oversight procedures that allow you to understand and verify financial information. This might mean reviewing original bank statements before they go to your bookkeeper and reconciling them yourself every month. And regardless of how much you trust your employees, set a dollar limit on the checks they can write without authorization. Additionally, use direct deposit for payroll to protect against check alteration.

Treat employees fairly

Even though it's important to establish controls, don't overlook the value of treating employees fairly. Many employees rationalize fraudulent activities because they feel underpaid or underappreciated. Make sure your pay scale is competitive by comparing it with prevailing wages in your area and adjust if necessary.

Respect and recognize your employees' contributions to your business, and enlist them in your fraud prevention efforts. Ask them, for example, to identify ways someone could steal and what they would do to plug the holes. Their perceptions as rank-and-file workers may be different from yours and, therefore, extremely helpful.

Small steps = big protections

Your business may be small, but implementing even the simplest fraud prevention and detection program can protect against big losses from fraud. And taking these steps may also improve your company's operations.

Fraud to watch for:

Affinity fraud

Con artists with an affinity for big swindles often find the best pickings among members of their own demographic groups, according to federal and state authorities. Exploiting connections of race, religion, age, politics, profession or other common bonds, some fraudsters prey on the unwary in scams that can involve Ponzi and pyramid schemes. When they do, it's called affinity fraud.

Keeping it in the community

Affinity fraud targets individuals, but it can hurt businesses when a big chunk of their workforce is affected. If your company employs a large percentage of immigrants, for example, they may be susceptible to fraud perpetrated by other immigrants and could, as a result, be left penniless. In addition to the effect such emotional trauma can have on company morale, it could make employees more susceptible to committing fraud of their own in an effort to recoup their losses.

Even people who usually are skeptical of such offers are more likely to let down their guard when the pitch comes from someone with a common background. In one typical case, Texas officials took action against a Latino-operated group that lured Latinos with promised returns of almost 10% per month for investments in nonexistent oil wells.

Making this type of crime hard to fight is the fact that victims are less likely to report scams involving these perpetrators. Many prefer to work within their community to try to resolve the problem.

No blind faith

You aren't immune, either. Not only could you be targeted as an individual, but the scam artists — including some of your employees — could seek contributions as part of your business's philanthropic activities. Don't be deceived into believing you can spot such scams. Many affinity frauds are recommended by friends, neighbors and colleagues.

To protect yourself, research any investment opportunity or fundraising organization that approaches you, regardless of who makes the approach. A duped individual may present the opportunity in good faith. Also, refuse to be pressured into participation before you're ready, and be skeptical if you're asked to keep an opportunity confidential or can't get anything about it in writing. If a suspicious investment offer comes via e-mail, forward it to enforcement@sec.gov for investigation.

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.

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

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.mcgoverngreene.com and let us know how we can be of assistance.

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