

fraud alert

year end 2005



When one of the pack goes astray

Fraud in family businesses

How far can you go in searching for fraud?

**Sarbanes-Oxley: Not just
for public companies**

Steer clear of abusive tax shelters

**Fraud to watch for:
Retail refund fraud**



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

When one of the pack goes astray

Fraud in family businesses

One of the things that make family businesses such appealing places to work is trust. That's also one of the things that make family businesses vulnerable to fraud. It may be difficult for family members to believe any of their clan would intentionally harm a company that benefits all of them, but it happens more often than you might think. And it takes only one lone wolf to damage or destroy an enterprise you and your family have spent years building.

Accept the possibility

Family businesses are no more vulnerable to fraud than other organizations, but their fraud prevention and punishment efforts can be hampered by loyalties and emotions that don't exist in other companies. One of the biggest obstacles to fraud prevention in a family business is simply acknowledging that someone in the family would be capable of initiating or overlooking unethical or illegal activities.

But like any other business, family enterprises must include a system of checks and balances that make it difficult for anyone to defraud the company. It may be awkward for one family member to exercise authority over other relatives, but someone needs to take charge and be willing to take a stand if or when issues arise.

Of course, the person in charge potentially could be the one defrauding the company. That's why independent auditors and attorneys are critical. Family businesses should look outside their immediate circles of relatives and friends to retain professional advisors who can be objective when assessing the company. Audited financial statements from independent accountants, in particular, both protect the business and supply peace of mind to its stakeholders.

If your company is large enough to have a board of directors, whether formal or informal, that board or advisory group should include at least one outsider who's strong enough to tell you things you may not want to hear. Business associations such as the Young Presidents' Organization (www.ypo.org) or the Entrepreneurs' Organization (www.eonetwork.org), along with industry-specific trade organizations, can be good resources both to discuss family business issues and identify potential board members.

In some extreme cases, members of all-family boards or officers have been known to work together to bilk their companies — something that's much more difficult to do when collusion requires the assistance of an unrelated board member.

Punish or perish?


Another problem family businesses might face is what to do if they find that someone in the family has, indeed, defrauded the company. While legal action is an option, it's one families rarely can bring themselves to pursue against one of their own — at least not at first.

If you find yourself in that situation, ask a trusted attorney or accountant to explain to the perpetrator the illegality and possible consequences of the fraudulent actions in an effort to stop him or her without further damaging the company. If such interventions don't work, however, you and other family members may have no choice but to prosecute.



Avoid blind trust

Sadly, just as it's more difficult to accept that the family closet is hiding a fraudster, it's also much harder to resist a loved one's pleas for assistance. In worst cases, families may have to choose between maintaining ethical professional standards and saving a loved one from scandal or punishment.

From a distance, the choice may seem obvious, but when it comes to family there are rarely easy answers. Objective professional advisors, nonfamily officers and board members, and a corporate culture based on trust — but not blind trust — can help prevent a rogue family member from harming what should be a source of mutual prosperity. 

How far can you go in searching for fraud?

Despite your best efforts to thwart employee theft and fraud, you suspect one of your workers may be involved in fraudulent activities. You'd know for sure if you searched the person's workspace, but can you do that without violating his or her right to privacy? Or are you committing an illegal search that will end any chance of prosecution or even expose you to a lawsuit?

Provide warning

Employers generally have the right to perform workspace searches but should approach them with care. Laws vary widely from state to state, so consult your attorney before proceeding. Most states, however, allow you to search company-owned computers, desks, lockers and other personal workspace equipment if your company policy clearly states you have a right to inspect its property at any time and if you have justifiable reasons for the search.

Similarly, you can monitor e-mails, phone calls and Internet connections if you have a well-communicated policy stating that electronic communications are to be used only for business purposes and that you reserve the right to monitor such communications. In fact, the American Management Association reports that more than 75% of major employers review employee communications on the job.

But just because you *can* do something doesn't mean you *should*. Perform a risk/benefit analysis every time you're considering a search, regardless of your policies. And search an employee's workspace only when you're reasonably certain you'll find what you're looking for and you have procedures in place to deal with what you find.

Don't risk a lawsuit

The biggest risk is a lawsuit claiming invasion of privacy, discrimination or harassment. While there's no constitutional right to workplace privacy, workers who can demonstrate they were justified in believing certain areas wouldn't be searched often have a strong — and potentially lucrative — basis for a lawsuit.

Unless you have justifiable reasons for the search, minority employees may claim discrimination if

they're singled out for searches. Justifiable reasons include investigation of workplace misconduct and retrieval of missing files, whether due to suspected misconduct or not. Even if your reasons are beyond reproach, document them before beginning a search.




Female employees may claim sexual harassment if a search becomes too intrusive, and anyone can claim civil harassment if there's any kind of physical confrontation. If the suspected employee is a union member, it's wise to have a union steward present during the search.

To further guard against claims, never conduct random searches or search an employee's body. Also, if your employees routinely lock their desks or use their own locks on lockers and other personally assigned spaces, you may risk overstepping your bounds if you search those areas.

Perform a risk/benefit analysis every time you're considering a search, regardless of your policies.

Proceed with caution

As an employer, you generally have the right to search your employees' workspaces if you make sure employees understand the need for such searches and you don't intrude in ways that could be perceived as offensive. The laws surrounding such searches are complex, however, and you should seek legal counsel before undertaking any search. 

Sarbanes-Oxley: Not just for public companies

Enacted following several high-profile accounting scandals, the Sarbanes-Oxley Act of 2002 (SOX) and related SEC and stock exchange rules hold publicly traded companies to stringent corporate governance and financial reporting standards. Privately held businesses aren't required by law to comply with SOX provisions. But as heightened sensitivity to financial irregularities becomes widespread, private companies may find it difficult to stay in business if they don't adopt at least some of the act's provisions.

Lending approval

Many financial institutions are asking closely held borrowers for independent audits when they apply for sizable loans. The days of loan approvals based on review or compilation statements are largely over. If you want a line of credit of \$15 million or more, in most cases you'll need to supply audited financial statements and prove you have internal controls conducive to proper financial reporting.

Your business probably will also need to have at least one independent director — someone who isn't a manager or employee. Depending on the size of your company, banks may even require that independent audit committees be in place to provide adequate oversight.

Costs and benefits

While such measures can prove costly at first, particularly to small companies that have no boards of directors, they may be cheap in the long run. In addition to helping ensure that financial doors remain open, effective internal controls and independent oversight can protect businesses from embezzlement and other forms of occupational fraud.



But these measures can be beneficial even if your employees are honest because you may be required to adopt some SOX best practices in the future. Already, public companies considering merging with or acquiring private firms are looking for businesses with sound corporate governance and financial reporting processes. Likewise, insurers, customers, auditors and even prospective senior managers may expect higher levels of SOX compliance from private companies. And, of course, if a private company is thinking of going public, SOX compliance will be critical.

Not-for-profits profit from SOX

Like private companies, not-for-profit organizations aren't required to meet Sarbanes-Oxley (SOX) requirements, but some are finding it advantageous to adapt those standards to their own operational practices.

Nonprofits have always emphasized transparency and active board involvement in their activities, but some organizations are taking things to another level. One, for example, sought resignations from all its board members so it could recruit new members to review audits and oversee fund raising.

While not all not-for-profits can or should go to that extreme, there's no question that independent auditors and board members are as appropriate for nonprofits as for their for-profit contemporaries. Document retention policies, whistle-blower procedures and improved financial reporting standards all can benefit nonprofits — keeping donors, clients and the public informed and confident the organizations are good stewards of the donations they rely on.

SOX menu

The good news for closely held companies is that you can largely choose which components of SOX to implement for maximum benefit and minimum expenditure. Even better, you have public companies' experience available to help you select best practices.

Establishing policies to avoid conflicts of interest and requiring proper financial reporting are good places to start. Ensuring that independent directors or audit committees are truly independent is also important. Additionally, you may consider the following best practices, either as short- or long-term goals:

- Prohibit or closely monitor related-party transactions.
- Appoint a compensation committee that includes at least one independent member to approve executive compensation packages.
- Establish procedures for employees to anonymously report any financial concerns, as well as the processes that will be used to investigate such reports.
- Work with two accounting firms, rather than just one, to separate auditing and other financial matters.

Some provisions are rapidly becoming standard operating procedure for *all* businesses, not just publicly held ones.

Feeling the effects


A 2004 Foley & Lardner study showed that 77% of private companies already are feeling the effects of SOX. Some of the most common measures respondents adopted included financial statements attested by the highest levels of management, whistle-blower policies, board approval for nonaudit services performed by auditors and corporate governance policy guidelines.



In most cases, such measures have been taken voluntarily, but some respondents also reported that pressure from board members or auditors influenced their decisions. They added that many of their new policies just made good business sense, and that their financial reporting improvements increased comfort levels for lenders, investors and customers.

*Insurers, customers, auditors
and even prospective senior
managers may expect higher
levels of Sarbanes-Oxley
compliance from private
companies.*

Smart business decision

While the changes may prove time-consuming and costly at first, companies are finding long-term benefits in improving their standing in the community, preventing fraud and reassuring key stakeholders. SOX may be optional for private firms, but compliance is likely to be a wise business decision. 

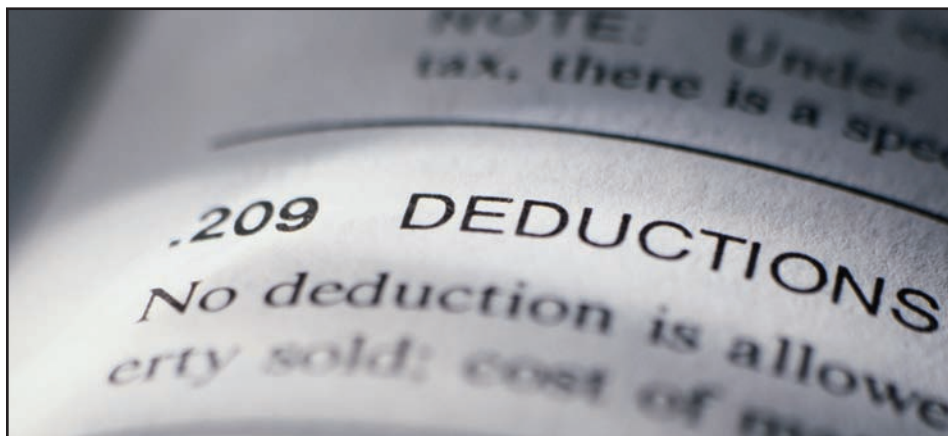
Steer clear of abusive tax shelters

As the year comes to a close, many business owners look for ways to save on taxes, making it the prime marketing period for purveyors of abusive tax shelters. Abusive tax shelters are complex transactions that have no legitimate business purpose and are used solely to reduce or eliminate tax liability in manners never intended or allowed under the tax code. However tempting the chance to save significantly on taxes, you should avoid such tax shelters at all costs.

Witting and unwitting victims

Unfortunately, abusive tax shelters aren't always easy to identify. Even reputable accounting, legal and tax firms may unwittingly market tax shelters the IRS deems abusive.

Some that have been uncovered appear less innocent, though. One major accounting firm, for example, marketed products that functioned as loss generators, allowing buyers to offset paper losses against other income, sheltering that income from taxes. In such cases, not only is the seller of the program liable for penalties, but the taxpayers who use the products are generally required to pay back taxes, interest and penalties.



As part of a comprehensive strategy to combat abusive tax shelters, the IRS requires that certain tax shelters be registered and that lists of investors be maintained by those who organize them. Anyone who participates in one of 30 "listed transactions" also must disclose their participation. These transactions include such activities as deducting employer contributions to employee benefit plans in one year for compensation earned after that year. The full list is available at the IRS Web site at www.irs.gov.

Avoid messy entanglements


How do business owners avoid becoming entangled in abusive tax shelters? First apply the age-old rule that if it seems too good to be true, it probably is. Abusive tax shelters are usually unsolicited — rather than a result of a business owner's request for assistance in managing tax liability. If someone approaches you with a proposal to make money through tax writeoffs, it's probably not a legitimate business investment.

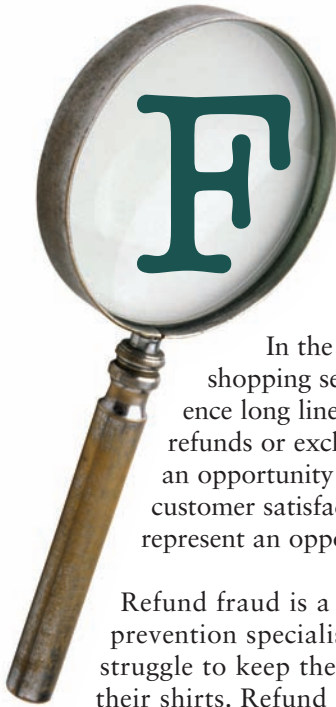
If there's no legitimate business purpose for entering into a transaction, there's no legitimate tax shelter.

Second, understand that legitimate tax advantages aren't available as one-size-fits-all products. Tax liabilities vary according to a business's financial situation, and no tax shelter is appropriate for every firm — even those being generically marketed as universal tax relief strategies.

Finally, look carefully at shelters that involve third parties such as foreign corporations, tax-exempt entities or entities with significant tax losses. If there's no legitimate business purpose for entering into a transaction, there's no legitimate tax shelter.

Shun the unknown

In short, if you receive an unsolicited offer to help you reduce your tax burden, look long and hard at the offer, the purveyor and the participants. Your trusted accounting and legal advisors can help you investigate the offer and steer you toward reliable and responsible tax strategies — strategies that are less likely to raise eyebrows at the IRS. 



raud to watch for: Retail refund fraud

In the weeks following the holiday shopping season, retail stores experience long lines of customers waiting for refunds or exchanges. Those lines represent an opportunity to significantly increase customer satisfaction, but they may also represent an opportunity for refund fraud.

Refund fraud is a significant thorn in loss-prevention specialists' sides as merchants struggle to keep their customers without losing their shirts. Refund fraud may be perpetrated by shoplifters who steal merchandise and then return it, customers who buy merchandise on sale and return it for full price, and employees who use receipts from previous sales to process refunds. Retailers selling electronics, computers and clothing are particularly vulnerable to customers who buy items, use them and then return them.



Some merchants, tired of watching profit margins slide, are tightening their refund policies. They might deny refunds to customers who repeatedly request them or who wait longer than the stated refund period to return merchandise.

While those practices are worth considering, preventing refund fraud should begin earlier. There are several measures you can take to guard against refund fraud:

- Require proof of purchase for all refunds.
- If you feel you must accept returns without proof of purchase, require full identification and information, including a photo ID.
- Provide cash refunds only if the customer can prove the original purchase was made in cash.
- Refund only up to a certain amount in cash and use checks to issue refunds for anything over that amount.
- When customers pay by check, wait for the checks to clear before issuing refunds.
- Provide refunds at a desk that's separate from cash registers.

Also watch for higher numbers of returns when particular employees are on duty. And make follow-up phone calls to verify that the customer whose name is on the refund slip is the same person who made the purchase and returned the merchandise. Not only does this help prevent fraud, it also allows you to track why merchandise is being returned.

In a competitive retail market, customer satisfaction is paramount, but retailers who don't take steps to curb refund fraud may find themselves losing more than customers. Refund fraud may be running rampant, but there's no need to let it run you out of business.

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

