



fraud alert

october/november 2005

**Nonprofits vulnerable
to fraud, but not
powerless**

An expensive oversight

**Expense account fraud can
cost more than you think**

**Don't let employees run laps
around your accounts**

**Lapping schemes a common form
of occupational fraud**

**Is Check 21 an
invitation to steal?**

**Fraud to watch for:
Under-the-table wages**



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

Nonprofits vulnerable to fraud, but not powerless

No business is immune to fraud, but not-for-profit organizations (NPOs) may by their very nature be more vulnerable than their corporate brethren. NPOs must operate on trust, and often on a shoestring budget. Frequently, their business, which can involve significant cash donations, is conducted by a mix of volunteers and employees who may be dedicated to the NPO's mission but aren't necessarily savvy businesspeople. Their boards of directors are usually volunteers who may be dedicated and savvy but may not have the time to devote to effective oversight.

Dangers lurk

While most frauds still occur in private companies, according to the Association of Certified Fraud Examiners' (ACFE) 2004 *Report to the Nation*, NPOs still get hit hard. The median loss to NPOs is \$100,000 (compared to \$123,000 for private companies).

Even more damaging for organizations that live and die by public donations is the loss of reputation that accompanies fraud. The media may give only lip service to NPOs under normal circumstances, but they're often only too happy to explore those organizations in great detail when there's a whiff of scandal. When that happens, donors become understandably leery of making charitable contributions.

Warning signs

There usually are warning signs that the atmosphere is ripe for fraud or that fraud is occurring. In fact, NPOs may unwittingly create such an atmosphere for themselves. Shrinking government subsidies and increasingly hard-to-obtain fund-raising dollars mean that NPOs must consider budgetary cutbacks. That may mean reducing the paid workforce and relying more heavily on remaining staff and volunteers.

The increased fraud risk is twofold. Staff cuts can breed resentment that may justify fraud in the minds of some. Second, such cutbacks too often are

accompanied by an erosion of financial controls — giving fraudsters more room to work. Similarly, tight budgets may cause board members and executives to focus on short-term fund-raising goals, allowing internal financial controls and reporting to take care of themselves.

Another danger specific to NPOs is off-site fund-raising. Without proper accounting supervision and control, benefits and other events can be open invitations to fraud. A paper trail of numbered tickets and receipts and other precautions will help curb many fraudulent impulses, but lack of oversight can make it difficult to determine whose hand was in the till — and how deep it dipped — when the event is over.



Prevention the key

Once it occurs, fraud can be difficult to spot. It is possible to stop it before it starts, though. The following steps may help:

Perform background checks. Distasteful though it may be to an organization devoted to doing good, you should perform background checks on employees and volunteers — including prospective board members and executives — who have financial responsibilities.

Require authorization. Requiring executive or board authorization for transactions over a certain amount — or, if an organization is small enough, for all transactions — will help control the money flow. Authorizing agents should also clearly understand how the transactions fit into the organization's operations.

Segregate duties. Ensure that the same person doesn't pay the bills, reconcile bank statements, control the safe and sign the checks. Divide duties and implement safeguards such as computer passwords to remove temptation.

Reveal and prosecute. NPOs that become victims of fraud often try to keep that news from leaking. Instead, make strong public statements, investigate fully and press charges against the perpetrators. Not only does this assure the public you're taking steps to protect their donations, but it also lets fraudsters know that criminal activities will not be tolerated. A full investigation should also reveal how the scam was perpetrated, allowing you to take steps to ensure that it never happens again.

Who's minding the mint?


One of the reasons that not-for-profit organizations (NPOs) appeal to those bent on fraud is that the monitoring and regulatory procedures surrounding them are not widely known. Unlike corporations or government agencies, where monitoring is often both vocal and visible, nonprofit watchdog groups tend to maintain lower profiles.

They do exist, however. A number of private organizations such as the National Charities Information Bureau (NCIB) monitor NPOs' performance, either to reassure donors that their money is being used properly or to keep the public aware of the NPOs' activities. These organizations also encourage NPOs to comply with prevailing standards.

Each state also has an office — often that of the attorney general — that is charged with watching charitable organizations. In addition to investigating fraud allegations, these offices typically maintain lists of registered NPOs and monitor compliance with their states' fund-raising laws.

The IRS, too, takes an interest in ensuring that NPOs meet eligibility requirements for tax-exempt status. Auditors in the IRS Exempt Organizations Division review the financial records of thousands of NPOs each year.

Don't ignore fraud

NPOs aren't always adept at finding fraud. The ACFE report noted that internal audits identified only 11.5% of fraud in NPOs, compared to 24% in other businesses. Such numbers, coupled with the fact that six in 10 NPOs said they have no internal audit departments, make it important that you employ external auditors to help you keep an eye on finances. While it's tempting to defer fraud control measures in favor of more urgent programming, it's a mistake you can't afford to make. 

An expensive oversight

Expense account fraud can cost more than you think

It probably seems like a relatively minor infraction to many employees: Write off the dry cleaning bill for a blouse stained during a business trip by adding the cost to the expense account. And, in truth, one small dry cleaning tab might not be such a big deal — if it stopped there. Too often, however, padding the expense account turns into a cottage industry for employees, an industry for which you may be footing a significant bill.

Know forms of fraud

There are as many ways to cheat on an expense account as there are employees willing to cheat, but four common methods are:

1. Mischaracterizing expenses. This involves legitimate receipts for nonbusiness-related activities. If Joe treats his buddy John to a birthday dinner, for example, that generates an actual receipt, but it shouldn't show up on Joe's expense account.



2. Requesting multiple reimbursements. This is a riskier scheme, but just as simple. If Joe wants you to pay for John's birthday dinner twice, he can just copy the receipt and turn it in on another expense report. Worse, he can attempt to be paid once for the bill, once for the receipt and once for the credit card statement.

3. Overstating expenses. When people overstate expenses, they request reimbursement for more than they spend. Changing a 3 to an 8 or a 1 to a 4 on a receipt is one popular approach.

4. Inventing expenses. This is probably the easiest way for an employee to get you to foot more than your share of the bill. All Jane needs to do is ask a cabbie for an extra receipt, fill it out with the numbers of her choice and turn it in for reimbursement.

These and other small expense account infractions can add up to outrageous sums. In one case, a senior vice president who traveled extensively for business was found to have defrauded his firm of \$30,000 over the course of three years by adopting a liberal definition of allowable business expenses.

In a 2002 study by Ernst & Young and Ipsos Reid, 7% of respondents said they knew people who inflated expense accounts. The study showed that junior employees under 35 who have been with their companies more than three years are the most likely to commit fraud. But managers tend to get away with larger amounts.

Pay more than lip service

In most cases, expense account fraud can be averted if companies implement fraud control policies and procedures and then enforce them. Too often, companies establish policies but fail to make sure they're followed correctly.

So once you have an expense report policy in place, communicate it. Be sure Susan knows her dry cleaning costs aren't reimbursable and Joe understands that updating his friends on his work schedule doesn't constitute a business dinner. This prevents misunderstandings and makes punishing infractions, when they occur, easier.


Also be sure a manager keeps abreast of employee business travel plans and other activities that might trigger expense reports. If someone submits a bill for a dinner in Toledo, his or her supervisor should have known about the trip before it happened. The supervisor should review every expense turned in, and require original receipts for everything. If a photocopied receipt is necessary — and sometimes it is — the supervisor should inspect it carefully for signs of tampering.

While computerized expense tracking software can't substitute for hands-on expense account reviews, it can help spot inconsistencies that develop over time. A computer program makes it easy to see if someone's expenses have soared in recent months or are noticeably higher than those of others in the department. A fraud-reporting hotline is also a good idea. It encourages anonymous reports of misdoings and signals that the company is serious about eliminating fraud.

*In most cases, expense
account fraud can be averted
if companies implement fraud
control policies and procedures
and then enforce them.*

Be reasonable

At the same time, be sure any antifraud policies you develop are reasonable. If your definition of reimbursable expenses is excessively narrow, employees may be more inclined to lie on their expense accounts to make up for out-of-pocket expenditures.

Finally, ensure that everyone in the organization is held to the same standards. Your CEO cannot be immune from scrutiny — especially because a CEO who cheats on an expense account may be perpetrating other forms of fraud, including falsifying financial records. 

Don't let employees run laps around your accounts

Lapping schemes a common form of occupational fraud

Lapping, or using receipts from one account to cover theft from another, is easy money for fraudsters and a relatively simple scheme to conceal. Not surprisingly, lapping remains one of the most common methods of skimming from company accounts. But you can prevent this type of fraud from damaging your business.

What lapping looks like

Lapping scams usually start small, with an employee pocketing a payment from ABC company and using a payment from XYZ company to hide the loss. As time goes on, however, the amounts get larger and the employee is forced to maintain detailed records to track the movement of money.

This house of cards usually tumbles when the employee makes an error. One commonly cited example is the man who stole \$150,000 by programming an elaborate computer scam based on 29-day cycles. It collapsed because he forgot that February normally has only 28 days.

As with any fraud, there are usually warning signs that can alert you before the lapping problem grows to epic proportions. These include:

- Excessive billing errors,
- Accounts receivable write-offs,
- Delays in posting customer payments,
- A trend of decreasing accounts receivable payments, and
- Accounts receivable details that don't tally with the general ledger.

Finally, customer complaints also are a warning sign of fraud and always merit investigation and follow-up.

Effective controls

Most of the time, lapping is a sign not only of a cash-strapped employee but also of a company with




inadequate controls. The man who stole \$150,000, for example, was the company's chief computer programmer and had unlimited access to customer accounts. To ensure lapping doesn't tempt fraudsters, take a few simple preventive measures.

Have someone review and compare every check that is deposited to the receivables ledger. This takes a little time but can offer a big payoff. Better yet, require that two people review the records. To be truly effective, the review should include the actual checks, not just ledgers. Because employees who are lapping may set up their own accounts in the company's bank, it's important for reviewers to have a list of valid accounts by bank name and number for authentication.

Another relatively easy protection against lapping is to closely monitor aging accounts. If you routinely send overdue notices to customers, make sure you pay attention to the responses. When customers say they've already paid an invoice, for example, follow up — you may be closing a door on a lapper.

It shouldn't be simple

It's not hard to understand why some employees might be tempted by the prospect of easy money — even if they may be caught in the long run. But with a little extra attention to detail you can make it difficult for lapping to occur in the first place. 

Is Check 21 an invitation to steal?

The Check Clearing for the 21st Century Act, or Check 21, which took effect in October 2004, is expected to speed check processing and cut banks' costs nationwide. But there is some question about whether it will also help financial institutions reduce fraud — or whether it will make fraud easier.

Cost-cutting solution

The law allows banks to process checks electronically — transmitting pictures of the checks they receive to issuing banks for approval. If a customer or another bank requires a paper document, the bank may use the electronic information to generate a substitute check that is legally equivalent to the original. The original can be destroyed.

Because banks no longer need to ship paper checks to other banks that may be thousands of miles away, they can dramatically cut expenses. By most estimates, this provision alone will save the banking industry an estimated \$2 billion a year. Check 21 also reduces the time required for checks to clear — putting an end to the “float” of one or more days before checks are deducted from their issuers' accounts.

Making digital images of checks available to customers online may be tantamount to sending them to criminals.

According to the Federal Reserve, banks are moving to electronic check processing slowly: Less than 1% of the 50 million checks that Reserve banks collect each day involve digital check images. Officials anticipate that will change over time, however, if only because banks are under pressure to reduce costs.

Prevention or encouragement?

Most observers agree that once banks have educated their customers and implemented the

systems they need to produce and process substitute checks, Check 21 will represent a significant advance in check processing. There is less agreement on whether the new law will also be an advantage in reducing fraud.

Some experts — including Frank Abagnale, whose exploits as a con artist were depicted in the movie “Catch Me if You Can” — claim that any additional automation of critical business processes opens new doors for criminals. They point to an end of traditional methods of identifying fraudulent checks because banks will no longer have the original paper documents to examine, or at least not for as long.

Making digital images of checks available to customers online may be tantamount to sending them to criminals. With a customer's user name and password, fraudsters




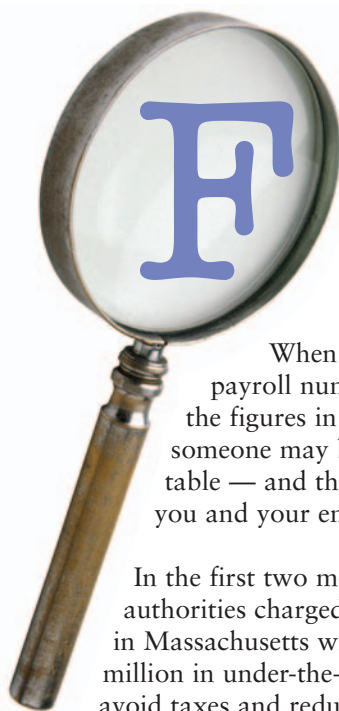
could get all the information they need to create counterfeit checks. They also could learn the average amount of a specific customer's checks, common payees and which check numbers are being used at the moment.

Others counter that such dangers are inherent in any online transaction. In its defense, Check 21 can virtually eliminate check kiting — a scheme involving writing checks on an account with insufficient funds. Every step in the two-to-three-day process of clearing paper checks offers an additional opportunity for fraud. By stopping paper documents at their transaction points, Check 21 ends many of those opportunities. Check 21 proponents do, however, acknowledge that the financial

industry needs to develop new, electronic methods of check fraud detection, which should allow much faster detection than in the past.

Opportunity to reduce expenses and fraud

The good news is that there will likely be plenty of time to strategize before Check 21 processing is the standard rather than the exception. The law merely gives banks the option of sending and receiving checks electronically. When they choose to adopt the technology that allows them to do so is a business decision that each bank must make for itself. Some foresight and innovation can help ensure that the transition reduces fraud as well as unnecessary expenses. 



raud to watch for: Under-the-table wages

When you're reviewing your payroll numbers, be sure you have all the figures in front of you. If you don't, someone may be getting paid under the table — and that can spell big trouble for you and your employees.

In the first two months of 2005, federal authorities charged two groups of employers in Massachusetts with paying more than \$33 million in under-the-table wages in an effort to avoid taxes and reduce insurance premiums. The business owners are alleged to have concealed true payroll amounts from the IRS and their workers' compensation insurance companies. If convicted on all counts, some of the defendants face possible sentences of up to 57 years in prison and \$750,000 in fines.

Even when payrolls aren't in the millions, the cost of paying with unreported cash can be significant. As an employer, you can be personally liable for all federal income and FICA taxes you don't withhold from your employees' wages. For every \$500 you pay in wages, you owe \$76.50 in withholding, making your potential liability

significant even without interest, late penalties, and possible criminal penalties that may include jail time. And that doesn't even begin to consider the \$50 fine for every W-2 form you fail to file, or the state penalties that may accrue.

It's true that compliance with payroll requirements is time-consuming, complicated and expensive. It's also true that, in some industries, under-the-table wages are becoming a standard business practice. In many cases, workers prefer to be paid in cash.

When those employees get caught, however, they are liable for income tax audits and payments — without any W-2s or pay stubs to prove how much they earned. They'll pay all the taxes they would have paid on reported income, and they may not qualify for Social Security, Medicare, unemployment or workers' compensation benefits.

All things considered, when it comes to payroll, companies are much better off putting everything on the table rather than attempting to save money by passing cash under it.

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

