



fraud alert

august/september 2003

Expense account padding:
Little rip-offs add up to BIG losses

Why asset misappropriation can spell ruin for a business

Getting ghost employees off the payroll

Frauds To Watch For:
Check kiting



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

Don't Let Workers Misuse Expense Accounts

From executives on down, anyone can be tempted to cheat on expense accounts. Traveling employees frequently may feel “self-compensation” is in order for all the time away. Others may cheat because they think it’s easy and nobody will notice — and in many companies, they’re right.

Big expense account policy loopholes let dishonest employees get creative. And managers who give expense reports just a cursory review don’t help. Encourage honesty by giving employees the benefit of the doubt when you can and by being fairly liberal in your per diem rates. But keep track of who’s claiming what and heed the signs of cheating. To flag possible expense account fraud, check these categories.

CLIENT ENTERTAINMENT

We’ve all heard of employees taking friends or family out for meals or other entertainments and charging the bill to their expense accounts, complete with fictitious client names. They might also alter cash and credit card receipts or submit false receipts from closed or non-existent establishments.

To fight back, set entertainment cost guidelines based on local prices. If a possibly phony business is listed on an expense report, call the business back. If possible, have employees get prior approval for client entertainment.

Issuing corporate credit cards can help. Require employees to use the cards when entertaining clients, and check the statements against the card receipts submitted with the expense reports. To encourage honesty and enhance client relationships, have employees record names, titles and addresses of clients they entertained, and send a letter to each thanking them for their time.

LODGING

Popular lodging scams include altering receipts and claiming to have stayed in a hotel after returning home, submitting a bill for a more expensive room than actually used, or bringing a guest along at company expense.

What you can do: Call around for local rates and set the budget. Check dates, account numbers and other details on hotel and credit card receipts. Stationery and format should resemble any

Nipping Expense Fraud in the Bud

Clear policies, a firm budget and careful checking are the keys to stopping expense reporting fraud. For starters, investigate all employees’ backgrounds before hiring them, and make it easy for your employees to anonymously report cheaters. When you’re reviewing expense reports:

Compare current to previous reports. Watch for a single transaction submitted on two separate reports with the credit card statement as backup on one and the receipt on the other.

Don’t accept photocopies without a good reason, and check for alterations when you do. An employee who consistently submits photocopies could be a repeat cheater.

At least yearly, summarize each employee’s expense reports and look for increases that aren’t justified by work assignments. Broadening the picture can make a suspicious pattern stand out sharply.

submitted previously from the same hotel, while handwriting on different receipts should differ. And, again, you can increase your control by requiring employees to use corporate credit cards.

AUTO EXPENSES

When you reimburse employees for mileage, how do you know the numbers are entirely business-related? If you suspect fraud, check back. Note whether mileage claims have been gradually — or abruptly — increasing, even though you haven't assigned the employee additional travel. When the employee goes on vacation and you assign someone else to his or her territory, compare the fill-in employee's reports to the regular employee's. You could also use the Internet to check mileage between locations.



*You can increase your control
by requiring employees to use
corporate credit cards.*

More auto-expense-reducing tips: To control suspiciously large gasoline bills, verify expense reports against credit card receipts for purchase dates, places and times, or get corporate gas credit cards. Go further by requiring toll and parking fee receipts to document expenditures.

AIR TRAVEL

Letting employees purchase air tickets can leave you open to some expensive scams. For instance, suppose an employee says he or she had to fly first class because no coach seats were available — but the employee actually bought a coach ticket and cashed in the pricier one? To stop this kind of

fraud, you can buy the tickets for employees and have them stamped “nonnegotiable.” If you purchase e-tickets, you’ll have a confirmation that the employee is flying coach.

If you can't purchase tickets, make sure employees actually use the ones they buy. If the employee didn't submit a copy of the ticket or purchase confirmation for an e-ticket and you suspect fraud, get one from the airline or travel agency. Verify that the ticket date matches the employee's scheduled travel date and the dates on hotel and ground transportation receipts. Finally, watch out for employees who rack up frequent flyer miles on one carrier, ignoring better deals at other airlines. Periodically compare prices and require that employees pick the most economical fares.

TAXIS AND RENTAL CARS

As every traveler knows, cab drivers hand out blank receipts on request. A dishonest employee might take a bus but submit a cab receipt. Or two employees might share a cab and both submit receipts.

To control cab expenses, go online to check distances between the travel points and call around for local cab rates. Some cabs now accept credit card payment, so employees can use corporate cards. If staffers regularly visit the same cities, establish accounts with taxi companies and have them bill your firm directly, reporting the name of the passenger, pickup and drop-off locations, and the total amount spent.

Although it's not easy, employees have been known to alter rental car receipts too. For instance, they

might get reimbursement for a more expensive car than the one they actually rented. Arranging for car rentals or requiring employees to use the company credit card can eliminate temptation.

LESS SELF-COMPENSATION

By establishing firm expense report policies, carefully going over each report and investigating discrepancies, you should be able to minimize fraud. For more information, please contact us. We'll review your situation and help you stop employees' cheating ways. 🕵️

Disappearing Act

WHY ASSET MISAPPROPRIATION CAN SPELL RUIN FOR A BUSINESS

Joe, the owner of a magic and novelty shop, contemplates his good fortune. Several months ago he hired a recent MBA graduate as the controller of his small business. In a short time, the new controller started handing Joe color-coded financial statements brimming with graphs and trend lines and featuring robust bottom lines. It appeared business was booming and profits skyrocketing.

With his mind at ease, Joe rewards himself with a two-week vacation in the Bahamas — his first real break in 15 years. While poolside, Joe is summoned to the front lobby to answer a stateside telephone call. He picks up the phone and Stan, a longtime vendor of Joe's shop, greets him. Stan informs Joe that the last vendor check Stan received has bounced. He would not be so concerned, but it is the third bounced check in the past six months. Stan wonders whether Joe is having financial difficulties and whether he needs to adjust the payment terms to help Joe through this rough stretch. Joe assures Stan that this must be a mistake and, in fact, tells him about the recent profit surge. "Good to hear that, Joe," Stan says. "But I got nervous when I saw the shop closed today."

"What do you mean closed?" Joe asks incredulously. "You know I have been open seven days a week since I started the business 20 years ago. I left my business associate in charge. You remember, the young fellow who drives that beautiful ... shiny ... red ... Uh, let me call the store myself and I'll get back to you." Of course, when Joe calls he hears the answering machine deliver the ominous message that yes, the store is closed. He later learns that the controller was not only stealing cash, but also writing checks to a phony business he had set up and, of course, altering the financial statements to present a rosy picture.



PRESTO! BANKRUPTCY

Unfortunately, this scenario plays out all too often these days. Joe is now the victim of an asset-misappropriation scam that will probably destroy his business or, if not, cause an insurmountable reputation loss. Asset misappropriation, or defalcation, includes both theft and misuse of company assets.

The Association of Certified Fraud Examiners' 2002 Report to the Nation concluded that asset misappropriation is rampant and certain business assets are much more susceptible to misappropriation than others. Fraudulent transactions involving cash and checking accounts are by far the most common. Almost 80% of the fraud cases reported involved asset misappropriation. Of that 80%, almost 90% involved cash.

The three most typical cash fraud schemes are skimming, larceny and fraudulent disbursements. Skimming, the easiest and most popular, involves taking cash from a business before it's recorded on the books. Skimming schemes are difficult to uncover because the cash never reaches a point in the recording process where it can leave a trail. Any employee who receives cash directly from customers or opens payments sent through the mail may be tempted to skim. And if, as in the case of Joe's deli, the fraudster is highly placed, it's easy to pull the wool over the owner's eyes — at least for a while.

New “vendors” might be your employees themselves routing money to post office boxes or even their own homes.

“On-the-books” larceny and fraudulent disbursements aren't nearly as popular because they're more difficult to sustain over a long period. When committing larceny, the guilty party steals cash that's already been recorded. Although the books will balance, the bank statement eventually won't,



so the bank often uncovers larceny or someone in the company does so when reconciling sales and cash. Fraudulent disbursements can involve setting up fake vendors to whom the fraudster writes company checks. In Joe's case, the schemes included cash fraud — probably skimming, fraudulent disbursements and financial statement fraud.

STOPPING SLEIGHT OF HAND

To head off asset misappropriation and especially skimming, separate duties so that the same employee isn't receiving payments, recording them and reconciling the books. Watch for inventory shrinkage, which can signal something wrong. Is your company's revenue declining while the cost of bringing in the revenue stays the same? Is your cost of sales inexplicably increasing? These could be signs of fraud.

For more hints that something might be wrong, pay close attention to customer complaints — they may lead you to major discrepancies between the customer's receipt for a transaction and the company's. If you can't find documentation of refunds or your documentation looks dubious, investigate further. Remember, too, that a shrinking ratio of cash sales to credit card sales, or cash sales to total sales, warrants suspicion on your part.

Do you know who your vendors are and where they're located? Be on the lookout, because new “vendors” might be your employees themselves routing money to post office boxes or even their own homes. Indeed, some fraudsters have even less imagination than they have shame.

SEEING THROUGH THE SMOKE AND MIRRORS

Finally, asking and seeing can be powerful deterrents to cash fraud. The best prevention is often the simple adage: “Show me the money.” Joe, you’ll recall, was enraptured by the shop’s

new and improved financial reports, but he learned that when something looks too good to be true, it often is. If you suspect asset misappropriation at your company, give us a call. We can check for warning signs and uncover any cash frauds that are weakening your bottom line. 📌



Fraud To Watch For: CHECK KITING MAY SIGNAL MORE FRAUDS IN PROGRESS

Although the bank usually bears the immediate losses, companies that fall victim to check kiting schemes often incur major cash drains as well. Here’s why.

Taking flight. Check kiting happens when a dishonest employee, working with at least two accounts at different banks, writes a check for funds not on deposit, deposits the check in another bank, then writes a bigger check on that account and deposits it at the original bank to cover the previous check and reap some extra cash, and so on. To maintain the scam, the kiter uses the approximate three-day float before the checks clear, and the banks’ willingness to allow withdrawals against unfunded deposits.

One checking account might be in your company’s name and the other in the kiter’s own name. Or, he or she could have an accomplice at another business to help use that company’s account. The checks usually get larger until one of the banks catches on and freezes the account.

An employee who’s embezzling company funds might kite checks so a cash shortfall doesn’t appear on your books. Or he or she might use some of the check-kiting proceeds to fund a more affluent lifestyle.

Reeling in the money. To stop check kiting, you and your bank must work together. Banks should monitor account activity and flag suspicious transactions, such as regular drawings against uncollected funds; frequent overdrafts or negative ending balances that are covered in a short time; or large, repeated deposits drawn on the same bank. Make sure your bank notifies you of any such red flags. And internally:

- Limit employee access to blank checks,
- Conduct regular check inventories,
- Control access to signature plates and store them separately from checks,
- Immediately reconcile checking account statements, then have a different person review the reconciliation, and
- Don’t let one person have access to blank checks, issue and sign checks, and reconcile statements.

Coming down to earth. Give us a call if you suspect your checking accounts are being misused or want to beef up your internal controls to prevent check kiting. We’ll be happy to investigate and advise you on the best course of action.

You Be the Exorcist

STOPPING GHOST EMPLOYEES AND OTHER PAYROLL FRAUDS

Dishonest employees are downright frightening. But it doesn't take ESP to stop them — just some increased oversight. Here are some spooky tales of payroll fraud and some suggestions for banishing ghosts and other evil spirits.

CONFRONTING YOUR FEARS

To protect your company, you must confront your fraud fears, which may take the form of:

Spectral employees. Someone with payroll system access can add ghost employees and pay them indefinitely. Outside perpetrators may get into the system by stealing user IDs and passwords. And ghost employees aren't always fictional. Legitimate identifying information could come from the fraudster's complicit friends or relatives. Or, the fraudster might keep ex-employees on the payroll and collect their pay.

Levitating paychecks. Here someone with payroll access and inadequate supervision may give him- or herself a raise without anyone else's knowledge.

Paranormal hours. Dishonest employees can inflate hours worked to earn extra overtime. Supervisors could even sign off on overtime in exchange for a portion of the money.

Supernatural commissions. Salespeople can falsify sales to boost their payments. They might inflate the value of a sale, steal a former employee's sale or just create a sale out of thin air.

Terrifying tax tricks. Outside payroll services often require companies to deposit payroll tax payments into a bank account one or two days before they're due to be deposited into the tax trust account. In a withholding tax scheme, an employee deposits the funds into his or her own interest-bearing account,

transferring them into the trust account on the due date. Even with today's low rates, interest on large tax withholding deposits can quickly add up. And if the fraudster doesn't shift the funds on time, the IRS can penalize your company.


Uncanny injuries. This scheme involves an employee faking a job injury and collecting workers' compensation benefits. He or she then works at another company while pretending to recover. Crooked physicians might issue false medical reports in exchange for part of the disability benefits or extra wages.



CLEARING THE AIR

To prevent payroll fraud, institute strict internal controls for payroll processing, computer access, and adding and deleting employees. Also, periodically review time records and paychecks to see that hours, salaries, tax withholdings and direct deposit data are accurate.

You may even wish to occasionally hand deliver paychecks or direct deposit stubs to employees. Last, use a firewall to block unauthorized users from your computer network.

Although they're not exorcists, auditors can dispel payroll-haunting spirits. If you suspect fraud at your company, please call us. 

McGOVERN & GREENE LLP

Certified Public Accountants & Consultants



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.

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

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

