fraud alert

june/july 2003

Join forces with your bank to STOP bookkeeper fraud

Don't FALL for domain name scams

Lapping schemes can rob you — and your customers

SURPRISE audits uncover more than meets the eye

McGOVERN & GREENE LLP
Certified Public Accountants & Consultants

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

Suspect Bookkeeper Fraud at the Bank?

HOW TO GET THE UPPER HAND

A dishonest bookkeeper can really deplete your bottom line. The cost of one instance of fraud to a private company with up to 99 employees averages $127,500, according to the *2002 Report to the Nation on Occupational Fraud and Abuse* from the Association of Certified Fraud Examiners (ACFE). And remember: Not all frauds are detected or reported.

Many bookkeeper fraud schemes involve bank transactions, and small businesses are prime candidates for such schemes because their limited staffs make it hard to separate fiscal responsibilities. One person handling all of a company's daily financial tasks can be so easily tempted that they wind up stealing. The solution? Heed any warning signs, find a bank that exercises prudent antifraud measures, and strengthen your internal controls.

BOOKKEEPER RIPOFFS OF CHOICE

Dishonest bookkeepers flourish in companies with poor or no internal controls, little direct supervision of accounting functions, and too much crossover of financial responsibilities. Following are some common bank transaction bookkeeper frauds:

Forgery. Shady bookkeepers may forge an authorized person's signature on checks made payable to themselves, to another person involved in the scheme, or to a fictitious person or company. They may even send a forged letter of authority to the company's bank, letting them sign checks, transfer funds between accounts or access detailed account information.

"Less cash" deposits. When depositing checks into the company account, bookkeepers may indicate a "less cash" withdrawal from the total. While some of that money may legitimately fund petty cash, a large portion finds a new home in the bookkeepers' wallets.

Phony bank accounts. If given the authority to change company bank accounts, bookkeepers may open a new company account that nobody else knows about. They can then periodically deposit company checks into the fictitious account.

Transfers between business and personal accounts. More online banking applications have increased convenience, but also the potential for fraud. Bookkeepers with access to company passwords can easily transfer money between company and personal accounts without ever leaving home.

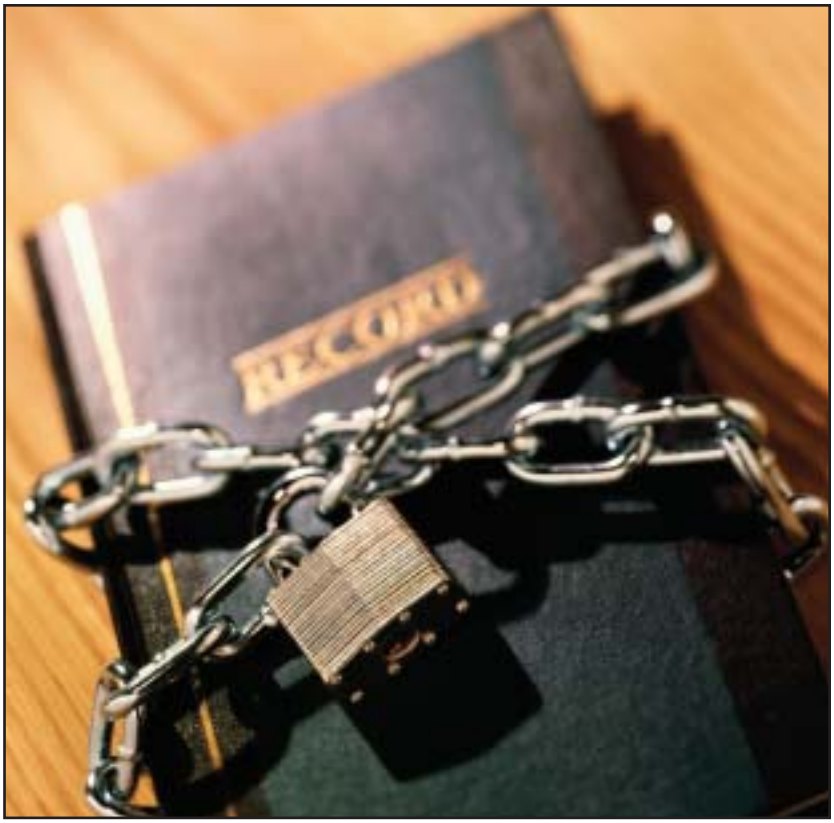
HOW YOUR BANK CAN HELP

It's essential that you get your bank's active support in stopping bookkeeper fraud. Before selecting a bank, check out its internal controls and choose an institution with strong fraud-prevention practices. Following are the most important controls.

First, banks should always maintain current valid signature cards. They should prohibit customers from individually changing or adding authorized signatories or from altering the original signature card. What's the most effective way to prevent signature card misuse? Maintain one card with all authorized signatories.

Next in importance is cross-referencing authorized business signatories with individual account holders. Your bank should do this when you open your account and whenever you change authorized signatories. It should immediately notify you if bank staff find that your bookkeeper, an authorized signatory for your company, also maintains a personal account at that institution. If the bookkeeper

can transfer money between accounts, a real temptation to commit fraud exists.



All banks must verify signatures to prevent unauthorized people from writing checks. Unfortunately, banks vary in how stringently they implement this control. Nevertheless, signature verification definitely helps ensure your bookkeeper isn't signing unauthorized checks against your company's account.

Along with verifying checks, banks often assign a relationship officer to business accounts. If you don't have one, ask for one. Relationship officers know your banking needs and whom you've authorized to conduct transactions and open or close accounts. Your officer should pay you frequent visits to get a first-hand look at your company operations. These routine visits can help detect any internal control problems and make it easier to spot someone attempting to open an account in a fictitious name.

WHY YOU NEED STRONG INTERNAL CONTROLS

Controls at the bank alone won't prevent fraud. Part of the responsibility is yours. Establish tough internal controls to fight bookkeeper fraud. Don't be too trusting — even of longtime employees — and remember that setting up and strictly following control procedures, though sometimes inconvenient, is a must for protecting your cash.

For starters, distribute bookkeeping responsibilities among several people. Don't let a single employee compile deposits, sign checks, make transfers between accounts and reconcile bank statements. The temptation to commit fraud in those circumstances can be overwhelming — especially to someone who's experiencing personal money problems you know nothing about. And to be doubly safe, designate someone who has no daily involvement with bookkeeping to reconcile the bank statements each month.

It pays to be vigilant and act quickly when you see signs of a cash shortfall. So regularly analyze your company income statements for any large fluctuations. These can signal potential fraud. The median time between the start of a fraud and its discovery is 18 months, according to the ACFE report. Most dishonest bookkeepers will continue until they hit an obstacle or are caught, and meanwhile the take keeps mounting.

Another key safeguard: Set up an annual CPA audit and discuss any income statement inconsistencies. Also consider occasional specialized fraud audits. A forensic accountant deals with internal theft every day and can quickly spot potential problems.

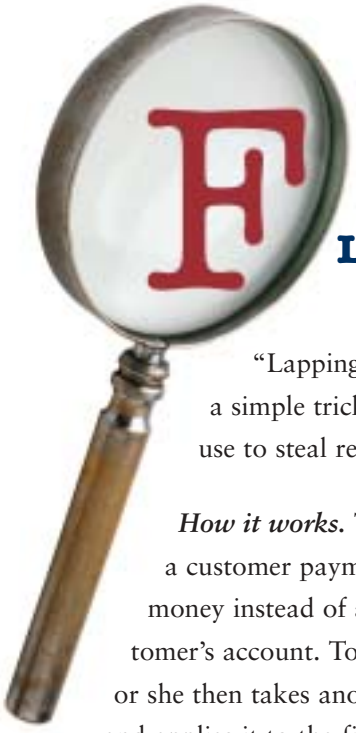
If your company uses online banking for transfers between accounts, don't give your bookkeeper the password. Instead, require the bookkeeper to get an officer's authorization to make transfers, or allow

only officers to transfer funds. Frequently change passwords for online account access.

Finally, don't be fooled by a sterling employee attendance record. Although it's wonderful for employees to enjoy being at work, an unblemished record isn't always what it seems. It may indicate the employee is committing fraud and can't afford to be out of the office for fear of discovery by a temporary substitute. If you suspect malfeasance, send your bookkeeper on vacation, call in a forensic accountant, and carefully review your books and records.

AN OUNCE OF PREVENTION

You can avoid bookkeeper ripoffs by choosing a bank that fulfills its control responsibilities and strengthening your own internal controls. If you'd like more information on how to keep your bookkeeping above board, please give us a call and we'll be glad to assist you.



Fraud To Watch For:

LAPPING STEALS FROM PETER TO PAY PAUL

"Lapping" customer payments is a simple trick dishonest employees use to steal receivables.

How it works. The employee receives a customer payment and pockets the money instead of applying it to the customer's account. To cover up the theft, he or she then takes another customer's payment and applies it to the first customer's account, and so on. As time goes by the employee constantly needs to repeat the fraud to prevent the employer from detecting his or her previous thefts. A lapping scheme can go on for years and become very intricate, so the scamster will sometimes keep an extra, private set of books at work that detail whose accounts he or she is manipulating and how.

Red flags. A marked slowdown in accounts receivable processing and in posting customer payments could signal lapping. Also look out for increasing billing errors and customer complaints. Most fraudsters just don't have the time or energy to keep the scam running and still work accurately and efficiently. Watch for an employee who seems to be keeping double transaction records, but beware of invading his or her workspace privacy. Consult your attorney before conducting any searches.

Prevention. It's simple: Don't let the same employee receive payments and record transactions. Trusting employees is fine, but they also need proper oversight.

To sum up, lapping doesn't take a financial genius to commit. Yet too many companies let it happen by maintaining weak financial controls, having the same employee perform too many functions and inadequately supervising their staffs. If you think lapping may be a problem at your business, please contact us for assistance. We can find out whether it's happening and, if so, help you put a stop to it.

Don't Fall for Domain Name Scams

PERSISTENT CROOKS TRY EVERYTHING TO CON COMPANIES

Your company's Web site address, or domain name, can become as valuable as a longtime trademark. Scam artists are well aware of this, so be on the alert for bogus faxes, mailings and cold calls urging you to register or renew your name.

EXPECT BRAZEN ATTEMPTS

Domain name piracy has been around for years and there are laws against it, but fraudsters are still open for business. The latest scam is to contact companies and offer unnecessary domain name registration or renewal. Here's how the deal could go down:

A pernicious phone caller. Someone may call and say another party is trying to buy your unregistered or expired domain name. Or, they might warn you they're going to put the name on the block where someone else will quickly snap it up. The renewal (or registration) deadline may be just hours away. Lacking the time to check your files for the name of your real domain name registrar, call them and investigate, you may just pay the bill, only later finding you've been taken.

A malicious mailing. In this scam, you receive an official-looking renewal bill giving you a short time to pay up before losing your Web address. Unless your staff is familiar with your actual registrar and renewal deadline, the bogus bill could easily get paid.

A fiendish fax. Also watch out for unsolicited faxes, which are illegal themselves. A Canadian domain name registrar ran afoul of the Federal Trade Commission (FTC) for sending bogus faxes warning small businesses that a third party had recently applied for a similar domain name. The only difference was the top-level extension (such as .com or .org). To protect their identities, many companies actually paid for the alternate domain name.

An evil e-mail. Some companies have received spam e-mails selling nonexistent domains such as ".USA." Other e-mails offer information on a potential domain registrar. But clicking on the link transfers your domain name to that registrar, resulting in expensive "renewal" invoices. This scam can also be perpetrated by mail or fax and carry the names of some well-known Internet companies. They may know your correct Web site address and renewal expiration date. But the fine print tells the real story: You're agreeing to a domain transfer.

BE VERY SUSPICIOUS

These scams are happening worldwide. The FTC offers help in its Consumer Alert publication, "What's Dot and What's Not: Domain Name Registration Scams," available at www.ftc.gov. Its advice: Steer clear of domain registrars that guarantee specific top-level domain names or offer preferential treatment in exchange for up-front fees. Also ignore anyone who sends you an unsolicited fax, and check out The Internet Corporation for Assigned Names and Numbers at www.icann.org.

DODGE THAT FRAUD

The key defense against fraud: Know your domain registrar and the terms of your agreement, and contact them before paying any bill. If you've been approached by suspected fraudsters or need help clearing your domain name, please give us a call.

For a Candid Look At Company Operations, Try a Surprise Audit

Ever consider a surprise audit? This time-tested technique for detecting and preventing fraud has taken on new importance in today's climate of strict corporate accountability. Adding hard-to-predict elements to the audit process can give you an uncensored view of your operations and spotlight problems. In fact, the American Institute of Certified Public Accountants (AICPA) is urging auditors to catch companies unaware during regular audits to bring any existing frauds to light.

Surprise audits incorporate a number of different accounting procedures to detect malfeasance from upper management on down. It's a sad fact: In many cases of fraud, a surprise check would have easily apprehended the fraudsters, but nobody bothered to do it. Especially if red flags indicating possible fraud have shown up in several regular audits, a sneak attack could be what's needed to clear up the situation.

TOP-LEVEL INVESTIGATIONS

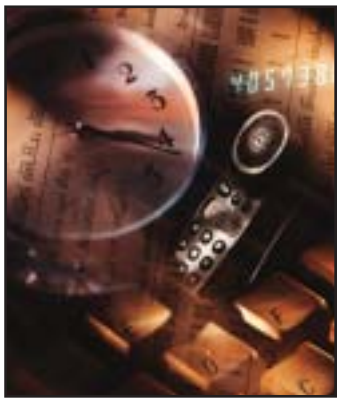
Say you suspect your company executives are committing fraud. A surprise audit can yield results the auditor might not get if you announce the visit. Traditionally, large financial statement frauds revolve around inventory, sales and accounts receivable. Examining certain accounts without warning prevents upper management from artificially inflating assets or revenue.

Inventory valuation fraud is one of the most popular techniques crooked management uses to manipulate financial results. If a company has multiple inventory locations, and management knows when and where auditors will conduct test counts, they have a chance to conceal shortages at places not scheduled for a visit. Going to locations and counting inventory without prenotification is a long-standing and effective surprise audit technique.

When you and your auditors feel comfortable relying on management's internal control systems, surprise audits are still a good tool for testing whether transactions comply with those controls. After all, it never hurts to step back and take a "snapshot" of your company operations.

DETECTION AND DETERRENCE

Surprise audits are just as useful in uncovering lower-level theft. Catching an employee off guard can be all it takes to uncover even a long-term scheme if the guilty party doesn't have time to shred, alter or hide records and other evidence.



Surprises can include not only when auditors start work, but also how they begin to do it. Say auditors usually start with cash at your company. You can bet any long-term ripoff artists know this and are counting on business as usual. They'll do what's necessary to conceal their activities when the auditor comes calling. Thus, an auditor may trip them up simply by starting with receivables or some other area.

In fact, surprise audits can both detect and deter fraud. Seeing others taken unawares may motivate employees committing as-yet-undetected frauds to abandon their illegal sidelines.

It's Not Rocket Science: The Story of Bob

Frequently used to uncover inventory, cash and accounts receivable frauds, surprise audits are most effective when the fraud perpetrators believe their thefts will go undetected. A simple example is the case of "Bob Doe," a recent high school graduate who gets a job at a photo kiosk in a shopping mall parking lot. After some basic training, Bob starts working and notices that no one is watching him.

One day Bob is short of money and steals $50. The next day he steals $50 more. No one notices anything missing, and over a few weeks Bob removes $700 from the booth. One day an auditor shows up unannounced, counts the cash and quickly detects the missing $700. When confronted, Bob admits that he temporarily "removed" the money without authorization. Bob gets fired from his job.

During his exit interview, Bob's employer asks him whether he knew someone would audit his work. "No," Bob replies. "Until the auditor walked into the booth, I didn't know there would be a surprise cash count." Obviously, neither Bob's fraud nor the audit involved sophisticated techniques. But if nobody had ever surprised him, Bob could conceivably have gone on stealing greater and greater amounts for a long time.

SIGNS OF THE TIMES

Surprise audits also help maintain corporate accountability in the wake of recent highly publicized scandals. More responsible than ever for uncovering malfeasance at client companies, auditors are at pains to demonstrate their professional skepticism.

The AICPA's Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit*, recommends that the engagement team test areas, locations and accounts that would otherwise not receive scrutiny. And, the standard says, the team should creatively design tests the client couldn't predict or expect. Specifically, they need to figure out how an employee might commit fraud, given the company's internal control systems. This involves stepping into a potential fraudster's mindset and imagining ways and means of stealing in a given area.

HIGH-TECH HELP

While simple fraud-busting methods continue to serve auditors well, surprise audits may also include high-tech sampling and computer data analysis techniques. For instance, specialized software can examine as many as 1,000 invoices quickly and in detail, including invoice numbers and to whom payments were made.

By isolating suspicious cases, auditors may spotlight schemes where, for instance, somebody submits phony invoices to a company's accounting department, which then sends payment to a post office box. A technology-sided surprise audit can also help uncover suspicious duplicate invoice amounts and invoice numbers.

A BOLT FROM THE BLUE

The element of surprise can go a long way in enhancing an audit's effectiveness. If dishonest management or employees take auditors' timing or procedures for granted, they may easily plan around an audit. But a surprise audit can stop them in their tracks. Give us a call if you think this technique would benefit your company. We'll discuss your situation and how a surprise audit might uncover what you want to know.

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