

fraud alert

august/september 2005

Pure fiction

**Bogus vendors may be
buried in your books**

**You may be at
risk for financial
statement fraud**

**Look inside to find
information security lapses**

**Ticking time bomb
Is your company vulnerable to fraud?**

**Fraud to watch for:
Bank deposit fraud**



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

Pure fiction

Bogus vendors may be buried in your books

A manager was on vacation when a question arose about a vendor payment he had authorized. The question was one the vendor could easily answer, but the company's CFO couldn't find a phone number in any records, and the vendor wasn't included in any telephone listings.

With that small beginning, the CFO uncovered a common fraud: Her company had been paying a fictitious vendor. The plan is easy to set up for someone with the authority to approve payments, and can go undetected for years. In one notable instance, the CEO of a trade association based in Washington, D.C., embezzled \$2.5 million over 13 years by receiving payments to phony consultants.

Employees wear vendor masks

While the consultants in the Washington case were real people — they just didn't provide services to the association — fictitious vendors are usually imaginary. The thief creates them and deposits payments to them in his or her personal account.

This scam is easier to perpetrate in companies with a large number of vendors, because the fictitious account simply gets lost in the sheer volume of paperwork. Even a small company can fall prey to the scheme, however, if the CEO is the perpetrator. In larger firms, middle managers may be able to set up fraudulent accounts.

Spotting the fake

Regardless of the size of your company or the position of the person perpetrating the fraud, there are likely to be some tracks for you to follow:



Missing information. Relevant and customary information missing from a vendor's profile is one sign. You expect to find phone numbers, taxpayer identification numbers, contact names and specific street addresses (not post office box numbers) in your vendors' files. When such routine data is missing or improperly formatted, you should investigate.

Embezzlers may create a company name that is similar to that of a legitimate vendor.

Vendor names. Embezzlers may create a company name that is similar to that of a legitimate vendor, or may use their own initials. (JFS Company, for example, could be the John F. Smith personal cash repository.) In any case, a fraudulent vendor won't be called Microsoft, Wal-Mart or any other widely known corporate name.

Account activity. A fictitious vendor will probably be an active vendor. Because the payoffs are proportional to the effort, fictitious vendors often don't send invoices for small amounts. The risk of discovery increases with every transaction, so fictitious accounts are more likely to involve fewer invoices for larger amounts.

Services vs. goods. Most often, fictitious vendors will supply services rather than goods, simply because it's easier. Occasionally, however, someone — most often a purchasing agent — establishes a fake company from which to order products. This scam usually requires an accomplice on the receiving dock to record receipt of the goods and simultaneously alter inventory records.

Other signs. These include:

- The absence of credit memos, because there won't be any billing errors,
- Prompt payments, because the perpetrator wants each transaction completed as quickly as possible,

- Similar invoice amounts, which will probably be just below the fraudster's authorization limit, and
- One invoice listing per check, rather than the more customary bundling of invoices for payment.

Finally, if only one employee (the fraudster) is requesting the company's services, that's a sign the vendor may not be legitimate.

Finding the perpetrator

If you suspect you're the victim of fictitious vendor fraud, look a little deeper to be certain you're paying only one sham company or person. Investigate if different accounts payable names have the same address or post office box, for instance.

Another way to trace perpetrators is to compare listed vendor phone numbers to employee phone numbers. In this day of cell phones on every hip, it's easier for employees to hide fake or "throwaway" numbers, but not every thief is sophisticated. You might run vendor identification numbers against employee Social Security numbers, too.

They can't hide

The good news is that changes in technology and improved internal oversight procedures make fictitious vendors easier to spot. When you have a sense that something's not quite right, investigate. Regardless of how devious the perpetrator and elaborate the scheme, vendor fraud can be uncovered. ¶

You may be at risk for financial statement fraud

Given the complexity of today's financial accounting environment, it's understandable when an occasional error creeps into a company's financial reports. What isn't understandable is when such errors are intentional. That's fraud — a form of fraud that costs businesses millions of dollars each year.

Understand revenue recognition problem

Financial statement fraud is defined as any intentional misstatement or omission in financial statements. But roughly half of all financial statement fraud is in revenue recognition, according to the American Institute of Certified Public Accountants. Tactics include recognizing revenue prematurely, reporting unearned revenue, reporting falsified sales or sales to related parties in excess of market value, and reporting incidental transactions as sales revenue.

One legitimate, but easily manipulated, accounting option involves pro forma earnings, which exclude one-time write-offs that aren't included when the year's profits are calculated. While there's nothing wrong with pro forma earnings statements, per se,



fraudulent managers can report the same write-offs for more than one year — distorting the company's value to investors. Another popular method is recognizing revenues in the wrong period — for example, claiming revenue from a product shipped on the last day of a reporting period when the shipment actually occurs sometime after the reporting period.

Examine corporate culture

The reasons employees become involved in fraud vary, but often financial statement fraud is intended to benefit the company rather than the individual. It

Question key managers' motivation

Because financial statement fraud is virtually impossible for anyone but key managers to commit, one of the first places to seek the potential for fraud is in the personal situations of those employees.

Affirmative answers to any of the following may indicate the need for further scrutiny:

- Have managers experienced past legal or regulatory problems?
- Is their personal net worth tied up in the company?
- Are they under pressure to meet financial expectations?
- Is their job security at risk?
- Do they promise to achieve unrealistic or ill-considered goals?
- Do they fail to correct known problems in internal controls when the problems arise?
- Do they have too much influence in the company's accounting principles?

most often occurs when managers are under pressure to achieve unrealistic earnings or to prove they are complying with financing covenants. Other reasons employees succumb to the temptation are to boost stock sales, negate unfavorable public perceptions of the company and earn performance bonuses.

So financial statement fraud thrives in a corporate atmosphere that encourages it; gamesmanship, arrogance, blind trust, ineffective or irresponsible controls, and simple loyalty all may play a role in an organizational attitude that pushes managers to exceed expectations by whatever means possible.

To uncover financial statement fraud, therefore, it is important to look past the statements and gain insights into the people who prepare them. An examination of top managers' backgrounds, their motivations and their influence in organizational decision-making may reveal the potential for fraud. (See "Question key managers' motivation.")

Scrutiny of the company's relationships with financial institutions, investors, external auditors, lawyers and regulators may also produce valuable perspective. One of the easiest ways to structure fraudulent transactions, for example, is to do so with related parties. Abrupt changes in auditing or legal firms may be a cause for concern if the reasons given for the change aren't clearly defined.

Search statements for answers

Of course, any search for financial statement fraud must ultimately focus on the statements. Most often, fraud surfaces when auditors look for changes in the statements rather than at ongoing practices and trends. Large changes in account balances or a sudden increase in receivables, for example, may indicate that something is amiss.

Other potential red flags include:

- Unusually rapid growth or profitability, especially compared to the rest of the industry,
- Inability to generate cash flow despite reported earnings growth,

- Managers' personal guarantees on significant debts,
- Constant "crisis" mode in operations, particularly when budgets aren't carefully planned,
- False, vague or incomplete footnotes that purport to explain complicated entries,
- A few large transactions that account for the bulk of an account balance, and
- Unrealistic account balances given the size and nature of the company.

Detailed examination of such occurrences may or may not show that fraud is being perpetrated. It will, at the very least, send a clear message that financial statement fraud will be uncovered should anyone consider it.

Improve financial oversight

To prevent financial statement fraud, improve your company's financial oversight and planning processes. This will make it less likely that a manager will be tempted to use fraud to help the company — and more likely that such efforts will be revealed before they can cause long-term repercussions. ⓘ

Look inside to find information security lapses

Despite all the headlines about phishers and hackers, most breaches of information security are internal. According to the 2004 Computer Security Institute/FBI Computer Crime and Security Survey, insider abuse of Internet access accounted for as much as 59% of financial losses due to misuse of computer systems.

The risk of outside attacks from such threats as viruses remains real, but a company focus on external security may inadvertently leave the door open for internal mischief. The good news is that strong information security systems can work; unauthorized use of computer systems and dollar amounts of reported losses have steadily declined since 2000, according to the survey.

Motivation breeds success

To be truly effective, information security systems must guard against internal threats as carefully as they protect against external attacks. The most effective antidote to internal information security breaches, according to the Institute of Internal Auditors (IIA), is motivation.

Senior managers, from the owner or CEO on down, must be convinced that security controls are a necessary expense in measuring, managing and controlling information processes so that neither internal nor external abuses are easy or profitable. Training staff to detect and report possible misuse of company computers can reduce the number and impact of incidences, as well as promulgate good security habits throughout the organization.

Information security is an expense that can yield a return on investment. Increased compliance can lower audit fees and insurance rates, while building security measures into programs can cut application and deployment costs.

Commitment to compliance


To be effective, your information security awareness program must be visible, understandable and memorable. Employees who don't understand or can't remember information security policy and procedures can become a weak link.

Deleting inactive user names and passwords reduces the chance they can be used for unethical purposes, while requiring employees to change passwords frequently minimizes the potential for individual account abuse. If you have computer security software, demonstrate how it works to all employees and modify their log-on messages to indicate the system is being monitored. You may even want to make information security compliance a part of every job description and included in every performance review — not just those of IT professionals.



Finally, develop an effective program to measure the information security system's success. Devise awareness measurement quizzes, for example, or require managers to conduct routine desk checks and password security reviews.

Big rewards

Make sure everyone in your company is aware of the information security policy and understands management is committed to enforcing it. Building security awareness into every operational, technical and development team project will ensure that employees view information security as important and valuable in protecting their business processes. 

Ticking time bomb

Is your company vulnerable to fraud?

Objectively assessing risk for fraud can be a difficult task for any company. While deeply ingrained policies and longstanding procedures may seem adequate, they may actually harbor opportunities for fraud. Virtually every company, therefore, can benefit from a risk assessment performed by a fraud expert.

What's the risk?

Fraud experts consider a number of factors when determining where a company is vulnerable. Generally, businesses with hard assets that are easily converted to cash, including tools, vehicles or other widely disposable merchandise, are more vulnerable to fraud and theft than firms that provide services or highly technical or niche products.

Another factor that increases the chance of fraud is the business's corporate culture. A climate of fear, domineering management, frequent overrides of internal controls and a perceived lack of response to rumors of fraud all put a company at higher risk of becoming victim.

A company's vacation policy may also encourage fraud. If personnel in key financial positions aren't required to take annual holidays, or if a vacationing employee's work is allowed to pile up undisturbed until the employee returns, fraud may result. Similarly, employees who work excessive hours because they don't delegate responsibility effectively may be a fraud risk — particularly if they are under pressure to meet budgets and market targets.

How easily someone could perpetrate fraud within existing operations is something else a fraud expert considers. If key areas are chronically understaffed, expense account claims aren't verified, important duties aren't segregated or transaction documentation is untimely or poorly organized, a knowledgeable employee can exploit these weaknesses.



Where's the money?

Fraud experts also look for financial warning signs that trouble may be looming. These include:

- Overly secret dealings with certain customers or suppliers,
- Large amounts of cash on hand,
- Missing or unexplained documents,
- Mismatches between profitability and cash flow,
- Insufficient justification for cash reserves, and
- Inadequate reconciliation of balance sheet accounts.


Excessive reporting requirements that leave insufficient time for data analysis, inadequate responses to questions from banks or auditors, lack of oversight to ensure that suppliers are appropriate, and inadequate internal reporting and management accountability can also open doors for fraudulent activities.

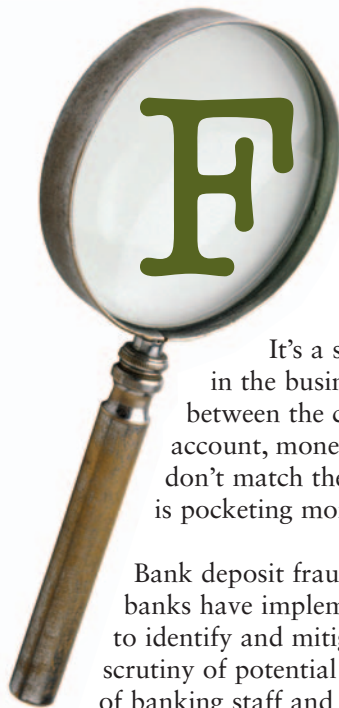
Finally, fraud experts generally interview people with detailed knowledge of how a business works (such as upper management) to help identify risks that aren't obvious, such as industry conditions, financing arrangements and commitments, technology changes, and competitive threats.

What's the solution?

Armed with as much information as possible, the fraud expert can then help decrease risk by suggesting procedural changes that will minimize the

potential for misappropriation of assets. Fraud experts can also help you decide what measures will be most effective in identifying fraud if it takes place and determine what procedures will be used to deal with the perpetrator.

Fraud risk assessment is critically important for any company, but too often internal assessments miss the forest for the trees. An outside expert can take a longer view to impartially calculate the areas of highest risk and then work with you to design and prioritize measures to address them. 



raud to watch for: Bank deposit fraud

It's a story heard much too often in the business community: Somewhere between the cash register and the bank account, money goes missing. The deposits don't match the receipts, because someone is pocketing money on the way to the bank.

Bank deposit fraud is pervasive enough that banks have implemented stronger measures to identify and mitigate it. More thorough scrutiny of potential employees, closer oversight of banking staff and sophisticated technology all play a role in reducing bank deposit fraud. But banks have no control over what your employees may be doing.

Follow procedures

To stop unscrupulous employees from perpetrating fraud, you must be diligent in monitoring the procedures that get your money to the bank. Make sure different people are involved in routine banking transactions. Don't let the same person prepare the deposit, enter it in the books and reconcile statements.

Also, be sure that at least two people prepare and deliver every deposit — and that they do so every day when cash is involved. Don't leave

deposits unattended before they go to the bank, either; lock them in a safe.

If possible, verify deposit transactions every day, too. Be sure original records of payments received match deposit amounts, and compare deposit slips to the actual amounts deposited. Online access to account information can speed this task. Finally, use monitoring and surveillance to detect evidence of altered records and to discourage would-be scam artists.

Look for the unexpected

Of course, a determined and sophisticated fraudster can sometimes evade even the best monitoring system. To unearth bank deposit fraud, look for the unexpected. Check if receipts, statements or deposit slips show signs of being altered, and be sure deposit receipts and statements match internal records. Also watch for deposits that aren't made in a timely manner — delays can indicate that someone needs time to steal his or her piece of the corporate pie.

Bank deposit fraud continues to grow, but routine controls and stringent oversight can keep it from exploding.

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

