

fraud alert

year end 2006



Don't let bust-outs break your bank

Sidling up to fraud

**Using indirect methods
to detect discrepancies**

How expert training can help employees stamp out fraud

ACFE Report

**Occupational fraud drains
U.S. companies' profits**

Fraud to watch for:

Identity theft center



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

Don't let bust-outs break your bank

The company seems like a dream customer: It pays promptly, has solid financial statements, a healthy bank balance and solid credit references, and wants to order more and more of your products.

Everything's going well, until the con artist running this gold-plated fraud decides it's time to move on, taking a significant amount of your merchandise without paying for it. You've become the victim of a bust-out — a business established solely to defraud reputable companies, including yours.

'Tis the season

Bust-outs aren't new, but they're sophisticated, well financed, well planned and, according to the National Association of Credit Management (NACM), increasingly popular. The NACM reported a record number of bust-outs in January 2006, when perpetrators capitalized on the holiday season frenzy to give the slip to harried companies that didn't realize what had happened until January.

While electronics and computer suppliers are among the most popular targets of bust-outs, particularly during the holiday shopping season, these con artists don't limit their activities to certain industries or times of the year. A Fortune 500 company that sells cosmetics or auto parts is just as susceptible to bust-outs as is a small firm that supplies headphones for digital music players.

Anatomy of a fraud

The fraud operates along predictable lines, but often is difficult for even the most experienced credit manager to detect. Typically, the con artist begins by creating a fake corporation and establishing limited

credit accounts with a couple of small vendors. By ordering small quantities of goods and paying for them as agreed, the fraudster builds good credit and wins favorable references.

Using those references and the positive credit history as bona fides, the bust-out firm orders as much as possible from as many vendors as possible. It then sells the goods, deeply discounting them for immediate cash payment, and either files for bankruptcy or simply vanishes. The original vendors are stuck with unpaid invoices and no products and, often, little hope of recouping their losses.

Take it slow

Unfortunately, in today's highly competitive business climate, bust-outs and their cash can look so good that eager sales reps and delighted CFOs may not be as vigilant as they should when checking credit. To avoid bust-outs, it's essential that you not let yourself be rushed. Swindlers may press for prompt credit approval, but fast-tracking credit checks or shortcutting procedures can be disastrous. In fact, you should regard unusual pressure for approval as a red flag.

Here are other signs that a business may plan to go for bust on your bottom line:

- The company requesting credit has a name that is very similar to that of a well-established firm.
- The income statement for the company reflects unusually large profits.
- The company shows a history of successive small orders followed by a sudden large order.



- A personal credit report on the principal doesn't reflect what you'd expect to see for someone who heads a company of this size — for example, a single credit card with a low balance, no mortgage or similar loans, and no open credit lines.

While not definitive indicators of a bust-out, these are signs that further investigation is warranted. One of the easiest steps to take is to visit the company requesting credit. The salesperson who landed the account or one of your managers should verify in person that the company actually exists and get a sense of its physical size. If the business later orders merchandise that doesn't seem proportional to the space available, you'll have some advance warning a potential scam is in the offing.

Regardless of whether you suspect fraud, always verify the information included in a new customer's financial statement. If the statement shows an unusually healthy asset-to-debt ratio, or has values for assets such as real estate that are difficult to substantiate, keep digging.

Also beware the bleed-out

Bust-out artists buy merchandise; bleed-out perpetrators buy companies. A close cousin to its higher profile counterpart, the bleed-out goes further by buying entire companies and then bleeding them dry.

Typically, a bleed-out operation begins when the fraudster buys a legitimate company with a good credit rating. The scam artist virtually always uses a long-term note and makes only one or two small initial payments to acquire the target firm. Once it has control of the company, the hemorrhaging begins. The bleed-out operator appropriates cash, sells assets such as vehicles and other items that are easy to dispose of, and unloads a great deal of merchandise at significant discounts.

Eventually, the original owners get their company back because the bleed-out artist hasn't paid the loan, but there's little left. Worse, the market has been flooded with goods offered well below break-even prices, and the once highly regarded company's reputation suffers.

If you're thinking about selling your company, verify all information a potential buyer supplies, including the principals' personal financial data and the trustworthiness of any references. And, remember: A company that looks too good to be true probably is.

Worth the wait

Thorough credit investigations can take some time, but they can save a great deal of frustration and expense. Bust-out artists may get tired of waiting for your credit approval, but legitimate companies shouldn't mind. 🕒

Sidling up to fraud

Using indirect methods to detect discrepancies

A routine audit at a small manufacturing company revealed evidence of asset misappropriation. The good news was that the evidence surfaced early enough to keep the scheme from causing devastating losses.

The bad news: There was no solid evidence of who was engineering the fraud. The owner, however, had his suspicions and called on a forensic accountant for help. Lacking direct evidence, the expert — with the help of the IRS — used a cash transaction (cash-T) analysis to expose the suspect employee's involvement.

This story is fictitious, but indirect methods of reconstructing income, such as cash-T, can be valuable tools in the fight against fraud. Lacking reliable financial records, forensic accountants can use indirect approaches to establish discrepancies between an employee's known income and expenditures.

Indirect may be best

Cash-T analysis compares individuals' known revenue sources (such as income from their jobs) with their use of those funds. If expenditures exceed income without a viable explanation, such as a spouse's income or proceeds from an inheritance, additional investigation may be warranted.

Other common indirect methods of reconstructing income include:

Net worth method. By calculating an individual's net worth (known assets minus known liabilities) at the beginning and end of a specified period, examiners can bring discrepancies to light. If an employee's net worth increases without a corresponding increase in known income, the difference may be approximately the amount he or she stole from the company.

Expenditure approach. A variation on the net worth method, this approach considers increases and decreases in an employee's bank accounts. Examiners subtract income from known sources from total receipts, adjusting for cash on hand or similarly explainable income. If receipts exceed known sources of income, the difference may be the proceeds of fraud. This method may be appropriate when the individual under suspicion is spending, rather than investing, the ill-gotten funds.



On its own, a BMW or trip to Barbados isn't evidence of fraud, but these details can help point investigators in the right direction.

Bank deposit method. With this method, experts examine funds that pass through bank accounts over the course of a year. Because it relies on a paper trail of bank deposits and expenditures via checks or other banking mechanisms, this approach may not reveal fraudulent income as readily as other methods.


Calling in the authorities

In many cases, accountants must work with law enforcement or tax officials to obtain access to the records needed for indirect methods of income reconstruction. There are several measures these experts can take to enlist such officials' cooperation.

Often, one of the first signs of fraud is an individual's lifestyle. Forensic experts simply look in the company parking lot to determine whether an employee's vehicle is commensurate with his or her known means. They also may alert owners to be aware of and report warning signs such as exotic vacations or sudden upgrades in wardrobes or jewelry.

On its own, a BMW or trip to Barbados isn't evidence of fraud, but these details can help point investigators in the right direction. When forensic accountants have enough indicators, coupled with other evidence that fraud is being perpetrated, they can enlist legal authorities to gain access to a suspect's personal financial records to help build a solid case.

Making discovery possible

Whether a forensic accountant works alone or in concert with legal authorities, establishing someone's involvement in fraud is possible even if that employee has incomplete or incorrect records. For businesses that are being victimized, that's good news. 

How expert training can help employees stamp out fraud

Would-be thieves are on notice. Businesses are tired of being fraud victims and are fighting back by training their employees how to recognize and uncover unscrupulous activities before irreparable damage is done.

Because many companies — particularly small businesses — lack the skills or knowledge to fight back, they're enlisting the help of forensic accountants. These professionals know what to look for and can provide comprehensive employee training that will give workers the tools to protect their companies against fraud and save significant money in the process.

Old scams, new help

While fraud perpetrators are imaginative when it comes to new fraud schemes, they often rely on time-tested methods or variations of old scams. After all, while the methods vary, all are designed with a single goal: to take money without being detected. CPAs know how to beat thieves at their own game and can train employees how to recognize and respond to scams.

CPAs can conduct on-site, broad-based training for all employees in the form of live presentations. Sometimes these experts use role-playing to help staff understand the various forms fraud can take, and how perpetrators think and identify their victims' vulnerabilities and weaknesses. More specific antifraud education can be provided based on employees' departments and positions.

On the front lines

Some of the internal and external fraud schemes CPAs are likely to educate employees about are:

Payroll theft. This comes in many forms, including paying phantom employees; manipulating time records; making and accepting unapproved pay rate adjustments; creating and accepting extra bonus or payroll checks; and committing W-2 or withholding fraud. To beat thieves, employees need to observe internal financial controls such as keeping a close eye on payroll-related records and expense accounts. A

CPA can review a company's existing controls and recommend improvements.

Check fraud. High-tech desktop printing equipment and laser printers are the only tools thieves need to manufacture bogus checks. Employees should know to look for warning signs such as the absence of a bank address or background design on the check, missing routing numbers, or odd texture to the paper.


Credit card fraud. Many thieves use others' identities and addresses to apply for and receive multiple credit cards and then go on massive spending sprees. Or they may be using stolen, altered or counterfeit credit cards. Employees should check that printed receipts match the name on the credit card and be alert to red flags such as misspellings on the card; alterations on the signature line; discolored, glued or painted cards; and cards that appear to have been flattened and restamped with different numbers.



Fraudulent charitable solicitations. If businesses aren't careful, charitable donations they think they're making to the police or fire department or other worthy causes may end up in someone else's pocket. Employees can be taught to ask for the full name, address and phone number of any charity and to contact the organization to verify its legitimacy before approving a donation.

Loan scams. Thieves call businesses offering loans at low interest rates, often asking for an upfront “processing” or “application” fee. Legitimate lenders, however, don’t require payment in advance of approving loans. CPAs can educate employees to check lenders’ validity through state banking departments. They also are likely to emphasize the importance of getting loan terms in writing — including the payment schedule and interest rate — before signing documents.

Sound advice

Companies can avoid a lot of headaches and protect their bottom lines by calling on CPAs to provide antifraud training. While fraudsters will never entirely abandon their efforts to profit at someone else’s expense, businesses can certainly make it harder for them to do so. 

ACFE Report

Occupational fraud drains U.S. companies’ profits

Dishonest employees cost U.S. organizations an estimated \$652 billion a year in fraud losses and are most often caught through anonymous tips, according to the Association of Certified Fraud Examiners’ (ACFE’s) 2006 *Report to the Nation on Occupational Fraud & Abuse*. Based on data compiled from 1,134 cases of occupational fraud that were investigated between January 2004 and January 2006, the report also found that the average U.S. business loses 5% of its annual revenues to this type of fraud.

In addition, the median loss in the ACFE study was \$159,000. Nearly one-quarter of the cases caused at least \$1 million in losses and nine cases resulted in losses of \$1 billion or more.



Types of fraud

ACFE identifies three major categories of occupational fraud:

1. **Asset misappropriation.** This involves theft or misuse of an organization’s assets. Examples include revenue skimming, payroll fraud and fraudulent invoices.
2. **Corruption.** In this case, employees use their influence wrongfully in business transactions to benefit themselves or other people. This type of fraud takes the form of accepting or paying bribes and engaging in conflicts of interest.
3. **Fraudulent statements.** Committed by falsifying a company’s financial statements, this type of fraud might involve recording fictitious sales or recognizing expenses in the wrong period.

Asset misappropriation — most often, of cash — is the most common of the three categories in the ACFE report, occurring in 88% of the cases reviewed. Conversely, cases involving financial statement fraud were the least common, but had the greatest financial impact. The median loss of \$2 million in schemes involving financial statement fraud was 13 times higher than the median loss for schemes involving asset misappropriations and nearly four times greater than the median loss in corruption cases.

The enemy within

More often than not, occupational fraud goes undetected for years before it’s discovered. Not

surprisingly, the higher the position of the employee committing a fraud, the greater the loss to the business. Those with significant authority have more access to business resources and, therefore, more ability to override controls that might otherwise disclose fraud.

The ACFE study found that fraud committed by owners and executives resulted in a median loss of \$1 million. That's five times greater than the median loss caused by managers and nearly 13 times higher than that perpetrated by employees.

As it did in previous years, the report also reveals that small businesses (those with fewer than 100 employees) experience disproportionately large fraud losses. The median loss incurred by small businesses was \$190,000 — higher than that of any other group in the study. These losses primarily involved employees fraudulently writing company

checks, skimming revenues and processing fraudulent invoices.

Not surprisingly, companies with anonymous fraud reporting hotlines suffered fewer losses than those without hotlines. In fact, fraud is more likely to be detected by tips than by other means, including internal audits. More than 40% of the million-dollar fraud incidents in the ACFE study were detected as a result of tips.

Sound advice

American businesses need to do a better job of implementing antifraud measures and controls proactively, the ACFE concluded. The only way to curtail occupational fraud is to take a stand against it by establishing systems that tell employees dishonest behavior won't be tolerated. ¶



raud to watch for: Identity theft center

Identity theft represents an ongoing, potentially dangerous threat to American businesses and individuals.

In response to this challenge, an alliance of corporate, government and academic entities has established the Center for Identity Management and Information Protection (CIMIP) at New York's Utica College.

Studying criminal groups

CIMIP, the first undertaking of its kind, will focus its research on critical issues in identity management, information sharing policy and data protection. In collaboration with the federal Bureau of Justice Assistance, an initial project will study current and emerging criminal groups that perpetrate identity theft and fraud.

Researchers will concentrate on the groups' operational methods in an effort to supply up-to-date, relevant information to law enforcement and help companies design prevention and detection strategies. They also will consider methods for developing stronger identity authentication systems.

That and other research at the center will focus on understanding the size and scope of the identity theft problem. Findings will be communicated through training sessions, symposiums, publications and the center's Web site, www.cimip.org.

An underestimated problem

Gary R. Gordon, professor of economic crime management at Utica College and a nationally recognized expert in economic crime, is the center's executive director. In introducing the new research center, he said one recent survey revealed that there have been more than 28 million new victims of identity theft since 2003. He believes, however, that the problem is probably much greater than such numbers indicate, because many incidents aren't reported or go undetected.

In addition to Utica, founding partners for CIMIP are LexisNexis, IBM Corp., the U.S. Secret Service and the FBI. Carnegie Mellon, Indiana and Syracuse Universities also are participating.

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

