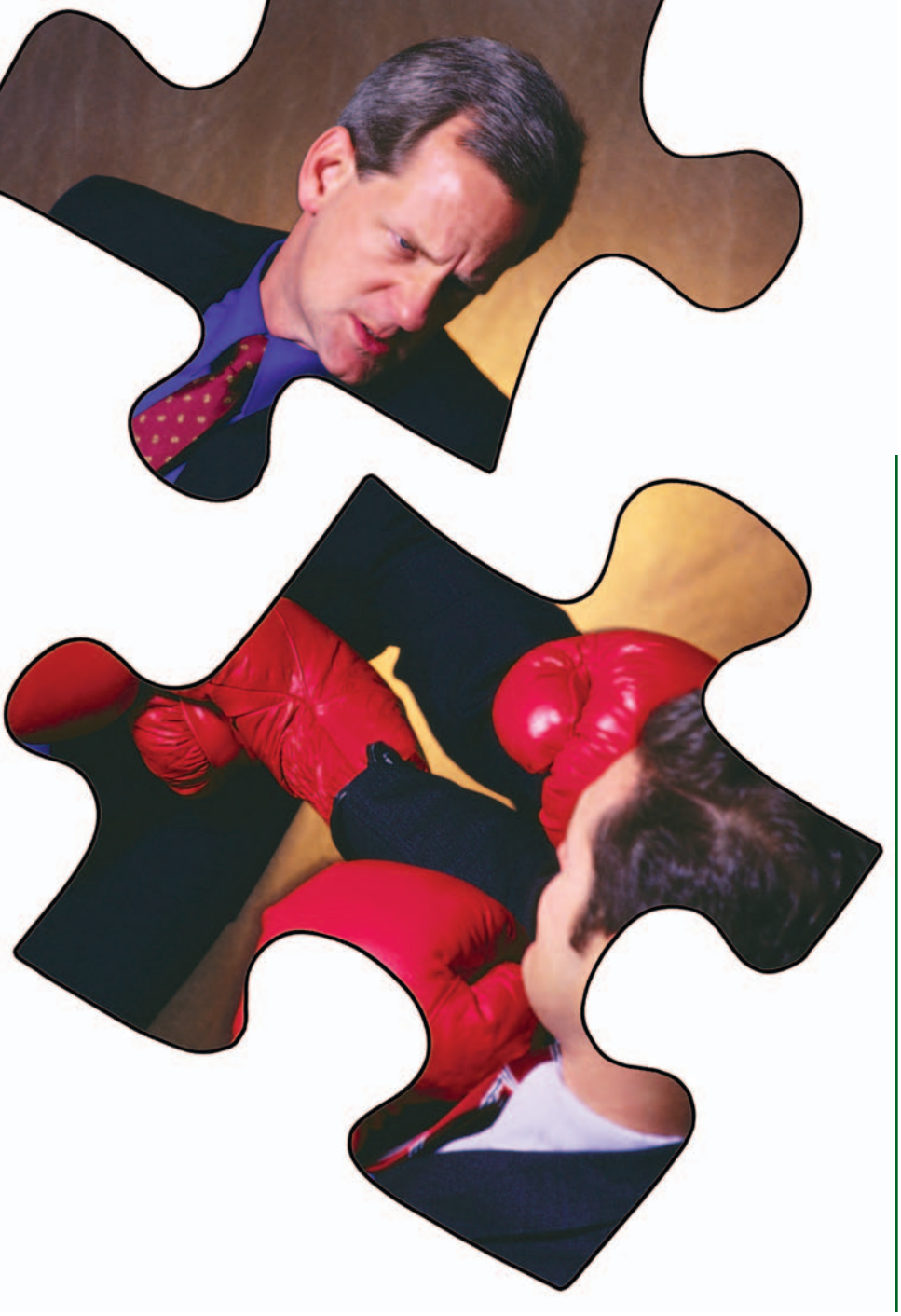

fraud alert

august/september 2004

Fighting the bust-out

Stay alert for fraud in accounts receivable

The fine line between gifts and kickbacks

How to spot insider loan fraud

Fraud goes global

McGOVERN & GREENE LLP
Certified Public Accountants & Consultants

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

Fighting the bust-out

Businesses can fight back if a crooked customer walks away — or busts out — from its bills. Bust-outs, deliberate bankruptcies to cover fraudulent credit use, may leave no paper trail, but forensic accountants can help attorneys assemble evidence for lawsuits against the swindlers.

A trusting supplier

Bust-out companies are created for the sole purpose of stealing from others. They may be short-lived, but they can do significant damage fast.

The following scenario illustrates how a bust-out works:

Business owner John Doe orders his first shipment of air purifiers and pays his new supplier up front for the entire purchase. Pleased with the volume of business, the supplier offers John generous credit terms. John reaches the credit limit without paying any outstanding invoices.

By the time the supplier becomes suspicious, John Doe has closed his company and cleared out the office. The supplier will never collect a dime from Doe, who is soon busy with a new company he sets up to sell the air purifiers he will never pay for. Sales are brisk, as the bust-out artist is able to sell the $200 purifiers for $50 — all profit, since he incurred no cost of sales.

Essential documents

When forensic accountants begin their investigation, they need all documents and communications with the customer before the bust-out, including credit applications and financial statements as well as credit background information.

Signed purchase orders leading to the bust-out are essential, as well as delivery receipts and packing slips. Other necessary documents include invoices and any checks issued by the buyer as partial payment. Also useful are names of individuals involved, such as purchasing agents, accounts payable and receiving clerks, and controllers.

The best time to fight bust-outs is before they happen. As an initial step in the due diligence process, verify the business location and get in touch with credit references. Ask how long the creditors have done business with the company.

Fraudulent business operations generally use short-term, low-rent locations and change location frequently. They often use mail drop addresses.

Investigate the address submitted to determine whether it is appropriate for that company's line of business. For instance, a residential address is an unlikely location for a wholesale, retail or manufacturing business.

Check resources offered by the National Check Fraud Center, www.ckfraud.org, or the National Association of Credit Management, www.nacm.org. Both have extensive databases combining information from law enforcement and regulatory agencies that fight white-collar crime.

Financial statement clues

Carefully examine all of the customer's financial statements. For a new business, check the stated worth and starting capital figures to be sure they are consistent.

Suspicious signs

When examining a new customer's financial statement, be on the lookout for signs that may indicate suspicious reporting. Here are some things to look for:

- A statement heavy on assets but light on debt. If it looks too good to be true, it probably is.
- Asset categories with values that are difficult to corroborate. An example is real estate.
- Accounts receivable entries in round numbers and those "due from officers." Analyze these figures carefully.
- Randomly dated statements. Financial statements are usually prepared at the end of a month, quarter or year — not May 17 or Aug. 21.

For a company with a history, check assets to determine if they can be confirmed by other sources, and analyze accounts receivable to see if the figures are consistent with the sales volume.

Ask the company's bank for the average balance for checking and any other cash balances. If bank figures don't jibe with numbers on the company's balance sheet, find out why.

In addition, check the credentials and reputation of the person who prepared the statement and of the firm that performed the audit. Confirm CPA accreditation with the appropriate state licensing board, and if the accountant is located in a different state, investigate to find the reason.

Victims can fight back

The best way to fight bust-outs is to keep them from happening, but victims can fight back. Forensic accountants work with lawyers to assemble and analyze the documents essential to successful lawsuits against perpetrators of bankruptcy fraud.

Stay alert for fraud in accounts receivable

Although accounts receivable can represent a significant portion of a company's assets, the processes associated with those assets are frequently regarded as low fraud risks. But fraudulent accounts receivable activities hold a very real potential for damage — to both a company's reputation and its bottom line.

In most organizations, the accounts receivable process consists of three steps: generating the invoice, recording payments and recovering overdue debt. When these steps are properly designed, implemented and monitored, employees will have a more difficult time pursuing fraudulent activities.

But even with the best processes, fraud is not impossible. So all businesses need to stay alert for signs of fraud.

Toppling a house of cards

Lapping, or crediting one customer payment account with money from another customer account, is probably the most common type of fraud by employees handling accounts receivable. It is also the most likely to be discovered, as it involves an intricate house of cards that is bound to collapse. But the longer the fraud goes undetected, the greater the liability to the company.

In lapping, the fraudulent employee transfers money from one company's account to cover the shortage created by theft from another company's account, then uses money from a third company to cover the shortage in the second company, and so on.

As such schemes become increasingly complex, they are more prone to topple. For example, simple calendar considerations defeated one computer-based scam. The scheme depended on computer transfers programmed for the 29th of each month. February, with its usual run of 28 days, was not taken into account in designing the fraud. When March 1 rolled around, the account transfers had not been made and the fraud was exposed.

Employees involved in both collecting and posting customer payments may engage in force balancing — posting customer payments without depositing those payments to a cash account.

To cover the discrepancy, the fraudulent employee overstates the total on the cash account so that it matches the accounts receivable postings. The receivables never age, but the company may see significant cash shortages if the scam isn't uncovered quickly.

Detecting write-offs

Another accounts receivable fraud scheme involves write-offs, which can be very difficult to detect when the perpetrator is someone with authority to adjust receivables accounts.

In this fraud, the employee writes off an account on company books as uncollectible while continuing to accept payments from the customer. A variation involves posting entries as discounts to cover skimming from customer payments. These discounts are generally small enough to avoid red flags that would prompt review.

Yet another way to conceal skimming from accounts receivable is through debits to aging or fictitious accounts. In this fraud, a payment skimmed from one customer is posted to that customer's account, but the corresponding debit is posted to another customer's account.

By adding the skimmed balances to accounts about to be written off, the employee records the stolen money as also written off, hiding the shortage from detection.

Spotting fraud signs

The good news is that alert businesses can usually spot signs of fraud in accounts receivable. Excessive billing errors, delays in posting payments, a trend of decreasing payments, slow accounts receivable turnover and customer complaints all may signal that something is amiss.

The better news is that businesses can take steps to thwart would-be thieves before fraud begins. One step is to be sure that no single person has too much authority. If one person is responsible for accepting customer payments, for example, someone else should be responsible for depositing the payments. And a third person should confirm that deposits match payments.

Fraud prevention efforts should not be limited to those with direct responsibility for accounts receivable functions. For example, the lapping that collapsed when there was no Feb. 29 was the creation of the company's information technology director, who had been given access to every computer and program in the firm.

In addition, be alert for signs of employee financial distress that could result in fraud. You may find that investing in financial counseling to help workers manage their money is a more acceptable expense than the cost of fraud.

Alert stance pays off

Even when companies follow sound methods for billing and collection, accounts receivable processes carry a risk of damage from fraudulent schemes. But businesses that develop programs to eliminate opportunity and spot signs of suspicious activity can reduce their exposure to fraud.

The fine line between gifts and kickbacks

How can you establish the fine line between a gift and a kickback? And what can companies do to prevent employees from accepting or offering kickbacks?

Kickbacks, illegal in the United States and many other countries, return a portion of the money exchanged in a business transaction as compensation for favorable treatment in the transaction.

Kickbacks may be disguised as gifts, travel, entertainment or cash payments. Other possibilities include promises of favorable treatment, hidden business interests, loans, and property transfers above or below fair market value.

Kickbacks vs. gifts

Gifts, gratuities or courtesies of modest value associated with ordinary business practices are usually acceptable. The key consideration is the intention of the giver.

An employee should not accept any gift offered with the intent to improperly influence business decisions — or that would give the impression of compromising the employee's ability to act in the best interests of the company.

The same integrity test should be applied in deciding whether to offer a gift to a customer or any other third party. You must take care to avoid not only an actual impropriety, but also the appearance of an impropriety.

Defining what is proper or improper with a specific dollar amount is extremely difficult; common sense must determine when the gift becomes extravagant or excessive. Employee handbooks usually set company guidelines for offering or accepting gifts, and professional organizations often provide their members with standards for gift giving and receiving.

For example, the Association for Investment Management and Research specifies in its chartered financial analyst (CFA) code of ethics that a CFA should restrict special cost arrangements and limit gifts to under $100 in value. In practice, this might mean that the CFA should pay for travel expenses rather than let corporate clients pick up the tab.

Tips from coworkers

Detection of a corruption scheme usually begins with a tip that comes from an honest coworker or a vendor who notices suspicious behavior, such as giving or receiving inappropriate gifts. Another potential giveaway is a pattern of lavish business entertainment.

Irregular habits in purchasing behavior can be a sign of trouble. Watch for repeated instances of ordering materials at a time other than the optimal reorder point and consistently placing orders with the same vendor.

Failure to follow general bidding policies also signals the need for a closer look. And if costs of materials seem out of line, the cause may be kickbacks in general purchasing.

Bidding irregularities

Kickbacks may come as part of the bidding process, in return for advance information about bids from competitors. Irregularities in the bid solicitation and submission process — for example, tailoring requirements in solicitation documents to fit the products or capabilities of a single contractor — may be signs of a kickback scheme.

Other signals of possible trouble include prequalification procedures restricting competition, bypassing necessary review procedures and a foreshortened bid submission schedule that allows only those with advance information time to prepare proposals.

Common sense

Kickbacks can take many forms. The line is not always clear between an acceptable gift offered with integrity and a kickback given as an illegal inducement for favorable treatment. But common sense can help in distinguishing between a modest and appropriate gift and an excessive, extravagant enticement.

How to spot insider loan fraud

When Smith, Jones and Wilson decided to start their own business, they had just one problem: They didn't have the up-front capital to launch it.

As a loan officer at the local bank, Jones was in a position to help. He approved loans to the other two partners, without disclosing to the bank that he, too, was involved. When the fledgling business began to struggle, the three recruited friends to borrow on behalf of their business.

Jones shepherded the applications through approval, using false information so the bank wouldn't see the real purpose of the loans.

The borrowers had no intention of repaying the loans. They allowed their names to be used, with the assurance that the business would repay the bank.

Jones and company's business didn't prosper, however, and when the third round of nominee loans became past due, the nominee borrowers went to the bank and disclosed the fraud.

Variety of methods

That story, taken from an actual court case, is unfortunately just one example of the methods swindlers use to defraud financial institutions.

Another popular approach is to make loans to fictitious borrowers, or to real people who have no knowledge of the loan. For example, a bank president made a series of loans to a fictitious person, securing the transactions with an alleged certificate of deposit held by another bank.

When the bank president left his job and one of the loans came up for renewal, the bank learned that every detail of the application was false, including the post office box that was the only address listed.

Bogus bonuses

Figuring more prominently in recent news reports have been insider loans by executives of major corporations, such as the two former Tyco executives charged with issuing themselves low- or no-interest loans and then forgiving the loans through an unauthorized bonus program.

Insider loans and securities fraud are among a host of possible crimes that can be committed by bank personnel at every level, but bank examinations are not geared to detect fraud. In fact, a trend toward more off-site examinations by state and federal officials means examiners are relying more heavily than ever on the accuracy of records provided by the banks.

No financial institution can ever be completely safe from fraud, particularly when the fraud is perpetrated by experienced, long-term employees who are trusted and have responsibility for certain areas or accounts. But banks can avoid making it easy to steal from them.

Internal controls

The first step to prevent fraud is establishing a strong system of internal controls that closes windows of opportunity for potential perpetrators. The initial line of defense is a hiring program that keeps people with questionable backgrounds from getting into the organization in the first place.

Once hired, every employee — from directors to tellers — must be held to a clearly stated code of conduct that is rigorously enforced. Regular internal reviews should include tests for the ability of

the institution's system of checks and balances to reveal insider loan fraud.

One early indication of insider loans may be addresses used on loan applications. If a post office box is the only address listed, for example, it is worth learning why.

One bank examiner noticed that several loans secured by real estate had been made to different borrowers with consecutive house numbers on the same street. Further investigation revealed the borrowers didn't own the real estate pledged as security.

Another red flag may be the lack of easily obtained essential information on loan applications. Inconsistencies like this or other suspicious information requires further investigation.

Follow up on suspicions

Simply reviewing files may or may not be enough to bring insider loans to light. Warning signs of insider loan fraud may come from several sources or just one. The key to eliminating it is to question anything that seems suspicious until problems are resolved. Also, look carefully at bank controls and practices that may open the door to illegal activities.

Fraud to watch for:

Fraud goes global

Like the economy, fraud is going global. As with legitimate business activity, global crime gathers a lot of its steam from the speed of modern communications. Heightened awareness of the twists and turns international con artists employ is the most potent defense against them.

International fraud varies in its particulars, but many of the swindles fall into the pattern known as the Nigerian advance fee scam. These schemes didn't originate in Nigeria, but their frequency in that country has attracted widespread notoriety and affected legitimate businesses there.

Most advance fee scams involve a message from abroad, either by regular mail, e-mail or fax. The letter writer usually claims that he or she is forbidden to open foreign bank accounts and asks the recipient to receive funds from an "over-invoiced" contract — offering a commission, of course. Agreement brings a string of requests for transaction fees or bribes to facilitate the funds transfer.

One variation is a letter from an allegedly reputable foreign bank that offers to act as a clearinghouse for venture capital in the country. The "bank" sets up a correspondent account in the United States, from which victims' money is immediately transferred overseas and into the waiting hands of the crooks.

Sale of crude oil at below-market prices is another tack. Or a foreign concern may offer to buy real estate that has been listed for sale, with the victim paying up-front fees to brokers who vanish as soon as they get the money. Other schemes involve disbursement of money from wills, contracts for delivery of goods or services, and conversion of hard currency.

It is no longer enough to defend against internal or national fraud. To be truly effective, today's fraud detection programs must be multinational, as well.

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