Forensic Focus

Insights on fraud detection and deterrence

FEBRUARY/MARCH 2009

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

105 W. Madison Street • Suite 406 • Chicago, IL 60602
www.mcgoverngreene.com

How to spot bankruptcy fraud

You've landed a lucrative new account, and the company already has placed several small orders with you, paying in full, on time. The customer is so happy with the products you've supplied that it wants to place a larger order, but has requested that you first expand its credit account.

One of its credit references is a Fortune 500 company, so it seems like a reasonable risk, right? Actually, there's a chance that you're about to become a victim of bankruptcy fraud. Your new customer may be the linchpin in a "bust-out" — one of the more common bankruptcy-related scams. As bankruptcies loom larger on the economic horizon, business owners must look closely before extending credit.

Don't be a victim

What's an effective way to avoid getting fleeced in a bankruptcy scam? Keep a vigilant eye on your credit, billing and collection procedures and activity. Most customers aren't out to defraud you, but tight controls won't hurt — and they may very well keep cash flowing.

Above all, be wary about extending credit to customers — particularly in a weak economic environment. If you do agree to provide products with longer payment terms, ask for collateral. Even a written personal guarantee from an owner can offer you protection if the business is being used as a bust-out.

When possible, get cash on delivery. If you can't do that, be aggressive about your billing and collection procedures. Legitimate customers will understand your request for payment, and potential scammers may turn to easier pickings.

Bust out of bust-outs

In a bust-out, fraudsters create a bogus company — often with a name similar to that of an established, reliable business — to order goods they have no intention of actually paying for. In fact, they plan to sell the products for fast cash, file for bankruptcy and leave you, the supplier, holding the empty bag.

In a variation of the scheme, bogus operators buy an existing company and use its good credit to order the goods. Either way, they sell the products they order below cost, for cash, and then file bankruptcy, writing off the amounts the suppliers bill.

To avoid becoming a bust-out victim, carefully vet businesses that were formed only recently. Also be wary of established companies with new ownership — particularly if the new owners seem to want to keep their involvement under wraps. Pay particular attention to customers that have:

- Warehouses stuffed with high-volume, low-cost items,
- Disproportionate liabilities to assets,
- No corporate bank account, and
- Principals previously involved with failed companies.

Although none of these conditions is absolute evidence of fraud, any of them may be a reason to proceed with caution.

Disappearing assets act

Bust-outs are far from the only bankruptcy-related scams unscrupulous operators use. In fact, the most common type of bankruptcy fraud is concealing assets, or fraudulent conveyance.

As its name implies, this scheme involves hiding or moving assets in anticipation of a bankruptcy. The owner of a business on the brink of collapse may,

for example, transfer property to a third party — or, most commonly, a spouse — for little or no compensation. The third party holds the property until bankruptcy proceedings have concluded, and then transfers it back to the business owner.

Alternatively, the business owner files for bankruptcy and then, with the court's approval, sells property below value to a straw buyer. The owner's relationship with the buyer isn't disclosed, but the buyer holds the property until the owner is ready to reclaim it at an agreed-upon price.

In either case, the goal is the same: to keep property and monetary compensation out of the hands of creditors. If you're one of the creditors the fraudster is attempting to defraud, the Federal Bankruptcy Code allows you to review asset transfers going back as far as 10 years. If you can demonstrate that any of the transfers were done to defraud creditors, you may be able to get them reversed and recover your share.

Stopping stays

Businesses that file for bankruptcy enjoy an automatic stay period, during which creditors may not press them for payment, file lawsuits against them or even call them to ask about future payments. The stay extends throughout the bankruptcy action, with two exceptions:

1. If someone is or has been involved in multiple bankruptcy filings, the stay lasts only 30 days, and
2. If creditors request that the stay be lifted because it's simply prolonging the inevitable — or in the case of fraud, giving the perpetrator more time to dispose of or conceal assets.

A company might, for example, file for bankruptcy the day before the bank is set to foreclose on its property. But a court could lift the stay and allow the foreclosure to proceed, enabling other creditors to resume their actions for payment.

Never say die

Fighting bankruptcy fraud typically requires guidance from financial and legal professionals. The best protection, of course, is prevention, but if you suspect one of your customers is trying to pull a fast one, contact your advisors as soon as possible. ■

Fraud aftershocks

Brace your business for disaster scams

Few things in life are certain, but when disaster strikes, the number of fraud incidents can be relied on to skyrocket. In the wake of a hurricane, tornado, flood, fire or earthquake, fraudulent operators are always quick to surface. Often, however, they carry warning signs to alert savvy business owners.

Construction con jobs

Construction fraud is particularly common following a disaster, in part because businesses focused on reopening as soon as possible may not vet contractors as carefully as they would in better times. That's what fraudsters are counting on.

If your company needs repairs after a disaster, work with your insurance company to be sure the repairs you're planning are covered. Your insurer will probably send an adjuster to evaluate the damage, giving you a ballpark estimate of what repair costs should be.

Next, take the time to obtain several bids. Review them carefully, bearing in mind that "special tornado offers" may be nothing more than come-ons. Be sure the bids specify exactly what work is included, all costs and a time frame for completion.

Beware of anyone who looks or acts unprofessional or offers to save you money by using materials left over from another job. You may be agreeing to shoddy components or unsafe workmanship. Before you hire anyone, ask for a state contractor license number and proof of insurance.

Then put everything in writing. Get a signed contract before work begins, and don't sign it until all the blanks have been filled. Don't pay in full until the work is completely finished — including site clean-up. And don't pay more than the amount in the contract — even if the contractor claims the cost of materials went up unexpectedly. Most states have laws regarding liens placed against property by contractors or suppliers. Before you make your final payment, ask the contractor to sign a Release of Lien form or a release of all liens, including subcontractor liens.

Many opportunities for fraud

Construction fraud garners the lion's share of attention after a disaster, but it isn't the only scam to be aware of. Also watch out for:

Vehicle repair fraud. These scam artists employ many of the same ruses as fraudulent contractors, and the safeguards against them are similar: Seek recommendations for reliable mechanics, check if the shop is accredited by the Motorist Assurance Program (MAP), and request pricing and warranty information up front. If prices are significantly higher than they were before the disaster, be alert for price gouging.

Fake relief workers. Ask to see photo identification cards from anyone claiming to work for the Federal Emergency Management Agency (FEMA) or the U.S. Small Business Administration (SBA). Don't be fooled by an official-looking shirt or jacket, and remember that FEMA and SBA inspectors don't charge for their services or solicit information such as credit card or bank account numbers.

Remember that FEMA and SBA inspectors don't charge for their services or solicit information such as credit card or bank account numbers.

Charity schemes. Your business may be ready to help others in need after a disaster, but you don't want to support con artists. Before contributing money or goods for disaster relief, verify the charity's legitimacy through the IRS, Better Business Bureau, your state attorney general's office or a nonprofit information site such as GuideStar.org. Be sure to ask the charity how it plans to use your donation.

Prevent a second disaster

Disaster sites may be breeding grounds for fraud, but you don't have to help make them fertile. With common sense and caution, you can avoid the aftershock of fraud. ■

Danger on the high seas

Shipping fraud is a byproduct of global business

The business world keeps getting smaller as companies expand their presence in overseas markets and add global suppliers. The shipping industry is one of the biggest beneficiaries of this new, worldlier outlook. Shipping fraud perpetrators are another.

Since time immemorial

There's nothing new about shipping fraud. According to the Insurance Regulatory and Development Authority, a ship owner in ancient Syracuse pocketed the money for a load of corn and then scuttled the vessel a few days later without loading the cargo — in 360 B.C.

Since then, businesses have become smarter about requesting written shipping contracts. 21st century shipping fraudsters, however, have more sophisticated schemes. For example, they might create false documents that claim a cargo has been loaded, and then pocket the money paid for the cargo and shipping. Cargos may be in transit for several months, so by the time anyone realizes what's happened, the fraudsters have taken the money and run.

Let the seller beware

Buyers too, can be shipping fraud perpetrators. A seller might, for example, make a shipment as agreed and forward a copy of the bill of lading to the buyer. The dishonest buyer uses the non-negotiable copy to create a new "original" document. The buyer then uses the fake original to clear the cargo when it arrives in port — thereby circumventing the legitimate bill awaiting payment. By the time the seller realizes payment is overdue, the spurious buyer and cargo are long gone.

One of the more insidious frauds related to shipping involves standby letters of credit. Issued by banks to secure underlying debt, standby letters of credit typically are used only if someone defaults on a payment — unless they're used for fraud.

Unlike commercial letters of credit, which require documentation such as bills of lading or commercial invoices for payment, these documents often require little more than a written statement of entitlement from the seller. Fraudulent operators can easily claim they haven't been paid and draw on the standby letter of credit. Although the issuing bank may require an invoice to prove the amount owed, it's virtually impossible to provide documents proving that a bill hasn't been paid. The bank has little alternative but to pay the requested amount.

Cover the bases

Multiple opportunities for shipping fraud make it imperative that companies look carefully before they leap into overseas shipping. In addition to conducting background checks on foreign business partners, require performance bonds from the companies' banks and request that an independent third party provide all documentation required for inspections and weight. It's also a good idea to hire a cargo surveyor to examine the cargo at the loading port and supervise the loading operation.

Don't forget to thoroughly vet your shipping company. Your investigation should include confirming that the vessel has enough capacity to carry your goods and that it's scheduled to call at both the loading and discharge ports. These precautions may help you avoid phantom ships — vessels chartered by thieves who change the ship's identity and destination after it has left port with a full cargo.

Another concern, as reflected in recent headlines, is piracy — particularly in the busy waterways off the coast of Somalia and in Asia's Malacca archipelago. Be sure you contract with an experienced shipping company that follows International Maritime Organization guidelines for preventing piracy.

Close the loopholes

As with any type of fraud, those who perpetrate shipping fraud are quick to take advantage of every opening. An expanding world market represents a growing opportunity for thieves, but with some care and due diligence businesses can avoid being hijacked on the high seas. ■

Put background checks to work for you

The first step in combating employee fraud is hiring the right employees. You can't rely on job applicants to tell you everything about their pasts, but you can do a little digging to ensure you're not hiring habitual thieves. Learning how to properly conduct reference and background checks can provide additional muscle to your company's antifraud program.

Be up front

The first step is to be as candid with your candidate as you expect him or her to be with you. Let prospective employees know you'll be checking references and performing a background check.

Then follow up. Ask former employers to confirm dates of employment, job titles and other resumé information, and then ask about the applicant's work habits and reliability. Many employers, fearing lawsuits, are unwilling to divulge more than factual information. But if you pay close attention on these calls, tone of voice can tell you how they really view their former worker. You should also verify education and certifications listed on the resumé. In addition to ascertaining whether the applicant actually completed the degree or certification, make sure no disciplinary action has ever been taken.

These are only the minimum procedures you should follow before hiring someone. If the position involves handling cash, operating company equipment, purchasing or other sensitive duties, you would be wise to drill down a little further with a background check.

Follow the rules

Background checks can provide invaluable information, but you can't go searching willy-nilly through someone's personal records. Obtain written authorization from the applicant, and find out from your state attorney general's office what state laws prohibit.

In some states, for example, you can look at an applicant's criminal history only if you're hiring for certain positions, such as a nurse or child care worker. But in most states, employers have the right to look at driving, credit, criminal and court records. Arrest records older than seven years can't be included in court records, but convictions may be reported indefinitely.

Whatever information you collect, make sure it's related to the job. If you're hiring a truck driver, for example, driving records are relevant. If you're hiring a bookkeeper, driving records probably aren't, but credit records are.

And keep in mind that you may not be able to use everything you dig up in making your hiring decision. If a job applicant declared personal bankruptcy five years ago, for example, that's not a valid reason to deny employment. If, however, the applicant has been convicted of bankruptcy fraud, you're probably justified in declining to offer him or her an accounts receivable position.

Recognize privacy

One area that's off limits to employers is an applicant's medical records — accessing and using these records in a hiring decision could have severe repercussions. Some workers' compensation information is public record, and you may use it, but only if the injury involved would interfere with the applicant's ability to perform

a certain job. And you are allowed to ask applicants if they are capable of performing a job.

Military records also are generally private, though the military may provide basic information such as rank, duty assignments, awards, salary and duty status without consent. And if you want more extensive information, you can ask an applicant's permission for the release of military records.

Use your discretion

Unless you're hiring for the CIA, you probably don't need to conduct a full background check on every person you hire. Reference checks, however, should be mandatory for every position — if nothing else, they'll tell you something about the applicant's honesty. But you can use your discretion in deciding which background checks to make, depending on your business and the position. ■

AICPA highlights forensics with new credential

Citing a growing demand for forensic accounting services, the American Institute of Certified Public Accountants (AICPA) began offering its fourth CPA specialty credential last September — Certified in Financial Forensics (CFF).

Sign of a specialist

The AICPA is the professional association for CPAs and sets ethical standards and U.S. auditing standards for private companies. Its new credential targets CPAs who perform fraud investigations. But the credential isn't limited to any one branch of accounting. In fact, it's being suggested for those who conduct computer forensic examinations, business valuations, bankruptcy reviews, and internal and external audits. AICPA members with five years' experience in accounting may seek credentialing if they meet requirements for forensic experience, lifelong learning or other related credentials.

Forensic credentials are available from other organizations, but the CFF is open to only CPAs. In addition, don't confuse CFF with the Certified Forensic Financial Analyst (CFFA) certification offered by the National Association of Certified Valuation Analysts or the other three AICPA credentials: Personal Financial Specialist (PFS), Certified Information Technology Professional (CITP) and Accredited in Business Valuation (ABV).

Demonstrated experience

Accounting professionals who seek a CFF typically already work to expose embezzlement in corporations, assess litigation damages and serve as Generally Accepted Accounting Principles (GAAP) experts in accounting fraud actions. They may include as clients attorneys, government agencies, corporations, criminal defense attorneys and prosecutors.

The AICPA, however, has said that three-quarters of the law firms they surveyed expected forensic accounting experts to have specialized credentials. Thus, the CFF credential can make CPAs more competitive in forensic accounting.

To earn the CFF designation, applicants must demonstrate experience with financial forensics and have accumulated at least 75 hours of lifelong education in the field. They may receive credit for related credentials such as Certified Fraud Examiner (CFE) or Certified Valuation Analyst (CVA). Although the AICPA is relying on experience and education for initial credentialing purposes, it's developing an examination for future applicants.

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

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 who 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**
- **Due Diligence**
- **Training & Seminars**
- **Electronic Discovery**
- **Financial Investigations**
- **Business Valuation**
- **Profit Recovery**
- **Government Contracts**
- **Contract Claims**
- **Forensic Accounting**
- **Asset Recovery**
- **Litigation Services**
- **Economic Damages**
- **Construction Audits**
- **Computer Forensics**
- **Internal Audit Services**
- **Healthcare Audit**
- **Intellectual Property**

CRAIG L. GREENE, CPA, CFE, MCJ

Craig is a leading fraud examiner and white collar criminologist. With over 30 years of experience, he frequently testifies in cases involving financial fraud, accounting, audit, and other disputes involving financial issues. Craig has led many corporate internal investigations focusing on financial statement fraud, corrupt payments, embezzlement and other occupational fraud schemes. He is an international lecturer on forensic accounting and fraud examination issues. E-mail: craig.greene@mcgoverngreene.com

CONTACT US AT 312.419.1961 OR VISIT www.mcgoverngreene.com
FOR EXPERT FRAUD EXAMINATION AND LITIGATION SERVICES

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