

Business Credit[®]

National Association of Credit Management

THE PUBLICATION FOR
CREDIT AND FINANCE PROFESSIONALS

February 2004
\$7.00

feature
article

Don't Get Your Pocket Picked

A new generation of computer-sophisticated perpetrators is using shell corporations, counterfeit documents and stolen identification to defraud corporations. Credit managers need to know what to look for and when to call for help.

BY Richard H. Gamble

Fraud is a big problem. The average company loses more than \$1 million annually to fraud, notes Gary Bares, president of Phoenix-based Verifraud, a fraud risk management consulting firm. In fact, between 15 percent and 30 percent of bad debt usually is due to preventable fraud, he claims. Typically, the perpetrators are a relatively small group of skilled professionals who victimize the same companies over and over again, year after year. They're clever enough to create credible fictional corporations that qualify for trade credit, but they're sloppy enough that they reuse addresses and phone numbers, work from the same city and have techniques that a fraud prevention pro can recognize fairly easily, Bares says.

The scope of the fraud problem is underestimated because many of the victims never know that they were stung, especially if the bust-out or shell company ends in bankruptcy. They just chalk it up to insolvency and write off the debt, Bares points out.

There are three principal types of fraud that victimize companies by exploiting trade credit, Bares says:

1. Business ID theft—criminals steal the identity of a valid, creditworthy company and use it to place orders that they divert to themselves. This type of fraud is relatively easy to detect and prevent with a little care.
2. Shell companies—criminals set up a phony company, give it a veneer of credibility to qualify for credit, place large orders and then disappear with the merchandise before the bill is due. These are often the most sophisticated fraud schemes. The shell company is “a ghost,” Bares says. “It’s a web site and a phone line. They don’t exist as real companies.”

3. Classic bust-outs—criminals acquire a legitimate company with a reassuring track record, boost the orders exponentially and then disappear before the seller can collect.

Fraud is easier to perpetrate today because the pace of business is faster, and electronic communication means that credit managers have fewer face-to-face meetings with apparent customers. Also, now that credit staffs have been cut to the bone, they have less time to investigate and confirm financials and references, Bares notes.

Consistent Lies

There’s no question that the thieves are getting smarter. It’s not rocket science, but it takes some skill and attention to detail to defraud trade creditors, says Doug Macfarlane, FBI special agent specializing in white-collar crime in the Los Angeles area. When you use bogus credit references, they have to know what you put on your application and showed in your financials. You need people who are prepared to tell consistent lies, he points out. Business practices are changing rapidly, and credit professionals have trouble keeping up, Bares warns. “They still take a one-dimensional view. They pull a credit report and rely on it, but they don’t look into where the information came from,” he says. Fraudsters have become experts at knowing just what credit pros expect before they provide a line and making sure that they have it. Some of the most dangerous fraud schemes come in with the cleanest credit applications, he cautions.

One customer of Tech Data Corp., Clearwater, FL, provided an audited set of financial statements complete with footnotes. “Everything a credit manager could want was right there,”

reports Scott Tilleson, CCE, director of regional credit. As an accountant, I admired the job they'd done. But if I'd checked out the accounting firm on the letterhead, I would have found that they didn't exist. We paid for expensive tutoring with that experience," he admits. "Now we check out any accounting firm whose work we rely on and talk with people who have used them and know they are for real."

Most of today's frauds are classic bust-outs with a new veneer of sophistication, Tilleson notes. "They give you everything you want. Most deadbeats try to hold back information, and that raises your suspicions, but the new perpetrators are very forthcoming with phony information."

Last year [2003] bust-outs were rampant, Tilleson reports. Perpetrators would find dormant companies with early establishment dates in the D&B database and then assume their identities and do a lot of buying before they busted out, he explains. Watch out for companies that on paper are many years old, but have only current trade references; and investigate those carefully before approving credit, he advises. They're probably hoping that old start-up date will get them past such close inspection, he adds.

In some cases, they will place just one order and clear out when they get it, but more often they make a few small orders and pay for them, then make a jumbo buy before they disappear, Tilleson explains.

One long-standing Tech Data customer in Texas sold his business, taking paper instead of cash for the sale. He stayed on under an employment contract, Tilleson recounts. The new owners immediately started placing large orders for a very different kind of merchandise than the business traditionally bought. "They were buying printer cartridges, not the usual sophisticated computer equipment. Those cartridges are easy to resell. And they were placing large orders." And then they were gone. The inventory was cleaned out. The new owners turned out to be ghosts. All their personal ID was phony. Police suspect that organized crime in Miami was behind it. The suppliers and the former owner were all left holding the bag; the former owner lost more than \$1 million.

Shell Game

Shell companies are particularly hard to detect. They may be legitimately incorporated, even getting valid business licenses. They typically have a reassuring website. Credit reports often are available—but unreliable—because too many credit reporting services rely on information submitted by the company itself, Bares says. Often there is a network of shell companies that serve as credit references for each other, so even if you have time to check references, the applicant seems solid.

But there are telltale signs that point to shell companies, Bares reports. One is zip code. The cleverest operate out of Los Angeles County, although some are starting to move to Las Vegas, he notes. Miami and New York are also suspicious sites. And they repeat their formulas. "I've seen the same group of

Ten Tips For Safer Sales

What can busy credit managers do to reduce the chances that their companies will be victims of fraud—and to increase the chances that perpetrators will go to jail if they are caught? Special FBI agent Doug Macfarlane, head of a white-collar crime unit in the Los Angeles area, offers these suggestions:

1. Make on-site visits when possible and ask questions. Look for logical business activity.
2. Ask for audited financial statements, and then confirm that a real accounting firm prepared them.
3. Be sure credit references are given in writing and signed.
4. Investigate further if a new customer tries to substantially increase its credit line quickly.
5. Don't accept faxes of checks as evidence that checks really have been prepared and mailed. You're never paid until the buyer's check has cleared his bank.
6. Be sure there's continuity in the credit department so crooks can't exploit a credit manager's vacation to get more credit than they should have.
7. Document phone conversations. This can be cumbersome but invaluable if a perpetrator is caught and brought to trial.
8. Keep all correspondence, including envelopes. Many crooks will be convicted of mail fraud if the evidence can be presented.
9. Talk to your peers and be active in trade associations. Fraudsters go after multiple victims. Whoever is trying to steal from you today, stole from somebody else last year. Check databases to see if a credit reference you have was used to defraud other companies in the past.
10. Watch for changes of ownership in an established company. Its track record may be solid, but the new owners may have a bust-out in mind.

people go through six or seven shell companies in the past five years," he observes.

One serial fraud had a series of shell companies based in Las Vegas, all with six-figure lines of credit from suppliers. All were registered to the same person, and all used references from California. They cheated a large group of suppliers out of \$300,000-\$700,000 apiece, Bares reports. The tip-off to a fraud investigator: all were operating out of a business services location. There was an address and a telephone, but no real companies.

One bust-out scheme went into action when the perpetrators paid less than \$100,000 to acquire a small company with a good credit record. Then orders skyrocketed. The company shot from reported sales of just a few thousand dollars a year to \$5 million. But they looked good on paper because they forged tax returns that showed net income in the millions of dollars, Bares reports.

Clever Counterfeits

Even when companies don't extend trade credit, they still can suffer fraud losses. One reason is counterfeit cashier's checks. New digital image and printing technology has made it easy for thieves to produce high-quality counterfeit cashier's checks and money orders, reports Joe Crowley, NACM's Asset Protection Group director. Credit managers may build in protection against bad checks with waiting periods, but they take a cashier's check or money order as the equivalent of cash, and that's not safe, he says.

Fraudsters will pay for a COD order with an apparent cashier's check, and someone typically will call to verify that the funds are available, explains Gary Bares, president of Verifraud, based in Phoenix. That's not good enough. There may be enough funds to cover the one valid check, but not the 50 copies that are being presented all over town, he notes. And unsophisticated delivery people make it too easy. "Sometimes perpetrators will take a regular check and stamp "Certified" on it; a driver will take it, not knowing any better," he recounts. "If you don't trust a company for open account terms, you shouldn't trust them for a large COD order either," he says.

Fraudsters also present counterfeit purchase orders, Bares reports. One counterfeit PO from a school district was so sloppy that "District" was misspelled as "Dostrict" and the seller took it anyway and got burned, he recalls.

Since even apparent cashier's checks are no guarantee of payment anymore, "We won't accept anything but an irrevocable letter of credit for some foreign sales," reports Chris Birdwell, credit administration manager for Pioneer Balloon Co., Wichita, KS.

A lot of times someone will call on a Friday afternoon, claiming to be in the purchasing department of a big company with a lot of locations. They need product—say three dozen laptop computers—shipped immediately. They'll fax or e-mail a copy of what looks like a valid purchase order, and the distributor will hurry to get the order shipped, Bares says.

Typically a shell company or bust-out artist will place a small order first, and see that everything goes well, perhaps paying by cashier's check. Then another order or two is placed to establish a pattern. Then they will show up late on a Friday afternoon, after the banks have closed, to pick up a large order, apologize for being late, and offer to come back Monday. "Most of the time, the seller will take the check as usual and trust that everything clears as promised and let them load the order," explains Chris Mathers, a Toronto-based vice president in the forensic practice of KPMG. The bad news comes Monday.

Red Flags

When you're given credit references with telephone numbers, don't just call the number you're given, Mathers warns. It could ring in any office, so you don't know whether what you hear is true or not unless you confirm independently that it is a real company and you're calling their real number. Also suspect anyone who is in a hurry to get a deal done and doesn't haggle over price. "The real customer usually will try to grind you down for every cent they can get," he notes.

One international crime ring linked to the Montreal mafia would bypass Credit, and ask Sales for a sample item, then order thousands of those items and send their own trucks to pick them up, paying for them with counterfeit certified checks, recalls Dennis Gaulin, chief intelligence officer of InfoLab, Brockton, Ontario, and a former credit manager at Black & Decker. Investigation uncovered a chain of more than 16 linked shell corporations, all operating out of the same industrial park and, of course, all owned by the same group. "It was a real labyrinth," he says.

Such complex fraud can mean trouble collecting claims against credit insurance, Gaulin warns. Insurance companies can insist on positive documentation of the fraudulent transaction, and that can be just about impossible to pin down when the scheme is complex and sophisticated, he notes.

One company that felt confident of its fraud-detection skills bought a list of 300 known fraudulent enterprises and discovered that they had forty of those companies among their accounts, Bares reports. Those accounts eventually cost that company nearly \$1 million in losses, he adds. "The challenge is how to get the attention of management if they think they don't have a problem," he says.

In the technology companies Bares works with, between 30 percent and 50 percent will have a fraud-minded account on their books at any time. "Stopping that fraud is a huge area of low-hanging fruit for companies that are trying to cut expenses. It's one of the biggest avoidable expenses that they have, in many cases," he says.

As the criminals get more professional and credit staffs get leaner, it's easier to make the case that you need a trained fraud prevention professional on the creditors' side, either as a staff member or working for a third party to which fraud detection is outsourced, Bares argues. "It's become a specialty; most of the fraud can be detected and prevented, but it takes training to spot it," he says.

Anti-Fraud Tools

For the fraud-prevention professional, there are a growing array of sophisticated tools—essentially large databases and good search engines, Bares reports. Accurint (www.accurint.com) is a good example, he says. The same perpetrators victimize many companies, so they leave a trail. If you know how to search, you can find a suspicious zip code or P.O. box, a suspicious phone number, a suspicious name on a check or application, he explains. "It's what law enforcement agencies use. You can put in an address or phone number and see who has had that address or phone number for several years. The databases are always being updated.

Legitimate companies show up where you'd expect them to. Shell companies just aren't there in the databases where they should be if they were real, Bares explains. "A legitimate business leaves tracks. When you don't find those tracks, you become suspicious," he notes. "Often what you are looking for is inconsistencies. A bit of evidence may not mean much in itself, but it can be part of a pattern that means fraud is likely," he says.

One of the newest threats is identity theft for principals in a business. The trade creditor requests a guarantee from the owner or owners and appears to get it, only it's not really the owner they're dealing with but someone who has stolen his or her identity and good credit history, reports Joe Crowley, director of NACM's Asset Protection Group (formerly called its Loss Prevention Group).

A lot of fraud also occurs within companies, underscoring the need for a thorough background check before people are hired, Crowley points out. One company unwittingly hired an employee with a history of petty theft. Then laptop computers went missing, he recalls. "They contained sensitive information, but fortunately the thief was looking for quick cash and just sold the laptops to people who didn't care about the information. If she had sold the information, it could have been devastating," he says.

Even without a criminal past, salesmen will get caught up in abetting fraud, Gaulin warns. "They'll get close to a customer and help overstate inventory in a floor-planning situation. And rather than accept returns, they'll move inventory from one customer to another and create fictitious credit and debit notes."

Credit Card Cons

While CDW, Vernon Hills, IL, sells PC products mostly to businesses, its fraud losses comes largely on credit-card purchases, reports Ken Ford, director of credit. On the corporate side, criminals do try to defraud CDW with shell corporations, but they rarely succeed, he says. "We investigate thoroughly, using D&B, directory assistance and public records. And when we get financial statements, we verify that the accountant who prepared them is legitimate," he explains.

Pioneer Balloon Co., Wichita, KS, had its brush with credit card fraud coming out of Nigeria. It could have been worse, but a customer in Florida alerted Pioneer that her credit card

number had been stolen. The company found that the card had been used to pay for two large shipments of party balloons to Nigeria and had the orders held at customs. A \$90,000 exposure was reduced to a \$7,000 loss, reports Chris Birdwell, credit administration manager.

Such large orders sent to Nigeria were not normal business for Pioneer. "The red flag was there, but we missed it," Birdwell admits. "Now we don't sell to Nigeria at all." And credit card buyers are routinely asked to read the number on the back of the card. "The only way you can know that number is to have the card in your hand," he explains. A thief who steals a card itself could give the number, but the more common theft of the number on the front of the card would be thwarted, he notes.

Technology, particularly the Internet, remains a powerful tool that can be used to prevent or perpetrate fraud. "I can be any company I want to be on the Internet. I can be a division of IBM, or 3M, or Microsoft," says Al Cameron, director of credit and loss prevention manager at Digital River Inc., Eden Prairie, MN, an e-commerce outsource provider. "I can get their information, duplicate it, work it into the necessary forms and order truckloads of steel, if I want to. And I can present a letter of credit from any bank in the world. Technology has given us that power. I have no idea whether my next door neighbor or the Mafia is ordering from me." To a computer, any name is legitimate until you tell it that the name is not, he observes.

Fraud can't be stopped, Cameron says. The best defense is to slow down the thieves and make it more trouble for them to defraud you than the merchandise is worth. If you put enough safeguards into your process, you can do that. He estimates that between 2,000 and 10,000 frauds are attempted every day, just over the Internet. Fraud is more prevalent in the B2C world, but the losses are greater in the B2B world, he points out. "They aren't stealing items; they're stealing shipments of items."

As long as fraud remains so lucrative, credit managers will have to stay on their toes to stop it, or at least see that their companies are not the victims.

Richard H. Gamble is a freelance writer. He can be reached by e-mail at gamble10@earthlink.net.