




PART IV

VERIFYING CREDITWORTHINESS

Chapter 12: Business Credit Fraud

Chapter 13: Making Credit Decisions



12

Business Credit Fraud

OVERVIEW

Predatory individuals perpetrate crimes of theft against companies by manipulating credit terms through misleading statements or actions which can cause significant financial losses. The real-life cases discussed in this chapter have been distilled into a variety of situations, circumstances and occurrences that, when identified, most often result in financial losses involving credit. These fraud warning signs are intended to serve as primary clues that a fraud against a company may be in progress.

The objective of this chapter is to provide a description of those known circumstances that most frequently reveal the trail of fraud and help credit professionals identify the steps necessary to protect their firms from financial loss through credit risk.



THINK ABOUT THIS

- : Q. What are the key the warning signs of business fraud?
- : Q. What can be done by a credit professional to identify possible fraudulent activity?



DISCIPLINARY CORE IDEAS

After reading this chapter, the reader should understand:

- ✓ Hallmarks of bust-out and same name scams.
- ✓ Why unsolicited orders are suspect.
- ✓ Why a large number of reference requests should be checked out.
- ✓ How the credit professional can be used as a reference in a fraud.
- ✓ Why unverifiable references, increased orders and unusual product mixes are suspect.
- ✓ How to spot misrepresentations.
- ✓ How to spot the warning signs of hidden ownership, the principal being unavailable, NSF and counterfeit checks.
- ✓ How to spot financial irregularities.
- ✓ What assets may be removed from a business.
- ✓ How to spot identity theft.

CHAPTER OUTLINE

1.	Bust-Out and Same Name Scams	12-2
2.	Unsolicited Orders	12-3
3.	Unverifiable References	12-3
4.	Large Number of Reference Requests	12-4
5.	Being the Credit Reference in a Possible Fraud	12-4
6.	Increased Orders and Unusual Product Mixes	12-5
7.	Misrepresentations	12-6
8.	Undisclosed Changes in Ownership	12-6
9.	Unverifiable Backgrounds of Principals	12-7
10.	Hidden Ownership	12-7
11.	Principal Unavailable	12-8
12.	NSF Checks Received	12-9
13.	Counterfeit Checks Received	12-9
14.	Financial Statement Irregularities	12-10
15.	Assets Removed	12-10
16.	Identity Theft and Social Engineering	12-11
17.	Fraud on the Rise	12-12
18.	Supplementary Material: Attack of the Doppelgangers	12-17

Bust-Out and Same Name Scams

Whenever the business economy faces a difficult time, thieves will find ways to use the problem to their advantage. There continues to be more variations on old scams and greater sophistication in newer scams. This being the case, companies that remain vigilant will be the ones least likely to be affected by business identity theft.

The definition of **fraud** describes the nature of bust-out scams and same name scams: *an intentional perversion of the truth for the purpose of inducing another to rely on it to part with some valuable thing. It is false representation of a matter of fact, whether by words or conduct, by false or misleading statements or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that a person shall act upon it to their legal injury.*

Bust-Out Scam

Spectacular corporate frauds led to the bankruptcies of companies like Enron and WorldCom and the bust-out scam continues to wreak havoc on businesses without the resources to shut it down.

Bust-out fraud, also known as **sleeper fraud**, is primarily a first-party fraud scheme. The fraudster makes on-time payments to maintain a good account standing with the intent of bouncing a final payment and abandoning the account. During the process, the fraudster builds up a history of good behavior with timely payments and low utilization. Over time, the fraudster obtains additional lines of credit and requests higher credit limits. Eventually, the fraudster uses all available credit and stops making payments. Overpayments with bad checks are often made in the final stage of the bust-out, temporarily inflating the credit limit and causing losses greater than the account credit limit.

In a classic bust-out, a company is contacted by someone with an offer to buy large quantities of merchandise on cash on delivery terms. The supplier delivers the goods in exchange for a check drawn on a business account. When the check is returned for insufficient funds, the customer makes apologies for the mistake and sends another check. Often, by this time, another truckload of goods is on its way, but subsequent checks have no more cash behind them than the first. The accounts are real but unfunded. By the time the supplier realizes they've probably been taken, the stolen goods have been sold and the company has skipped out or disappeared.

Same Name Scam

Since the beginning of credit ratings, fraudsters have taken advantage of systems designed to rate business's creditworthiness. To illustrate how the same name scam works, consider that there is a reputable business with an excellent credit rating in Detroit named Detroit Distributing. The enterprising fraudster knows that credit professionals don't always order credit reports for businesses with excellent credit ratings or particularly when the dollar amounts are relatively small.

The fraudster sets up an office or warehouse under a similar, if not identical, name to Detroit Distributing. In this case, the new business is called Detroit Distribution and is located in Detroit. The variation on the name is a very subtle difference, and will probably not be noticed by the majority of suppliers who receive orders. Most credit departments have a credit scoring system that allows orders under a given level to be shipped, depending upon the credit rating.

The fraudster proceeds to place a number of small- to modest-sized orders using the name Detroit Distribution. Unwary suppliers, finding the excellent rating of Detroit Distributing, ship without a thought. By the time the invoices come due a month later, the phony operation is long gone.

Upon further observation, most credit professionals will point out that there is a flaw to this scheme. Suppose the supplier already sells to the real Detroit Distributing and sends the invoice to the real company. Immediately upon receipt of the invoice, the real company's purchasing or payables department will likely call the supplier and point out that they never ordered the product in question. And, should the supplier review the ship-to address, they may find that the shipping address is not connected with the real Detroit Distributing. The best way to trip up a potential same name scam is for the credit professional to pay attention to detail; it simply won't work if addresses are verified.

Unsolicited Orders

One sign that something may be amiss is an unsolicited order. Generally speaking, no matter how good a product, the sales force needs to work hard to come up with business. When an order arrives from an unsolicited customer, it is often a warning sign of fraud.

A company may receive unsolicited orders in any number of ways, but they generally arrive online, via phone or at a trade show. The definition of an unsolicited order can be tricky. Many companies receive the vast majority of their business via unsolicited orders. For example, catalog businesses receive calls soliciting their goods routinely. Sometimes, as a result of a presence at a trade show, orders increase from unknown sources. As a credit professional, the questions to ask are: (1) how common is an unsolicited order and (2) is there a rational explanation for the order? Does it make sense?

Another clue is the relationship between sales and the customer placing the order. If the customer seems to be trying just a little too hard to give what is normally looked for; it is time for the credit professional to back off and be more careful. The key statement to remember is the often quoted, "If it seems too good to be true, then it probably is."

Unverifiable References

One of the foundations of the credit investigation process is the credit reference. The theory behind reference checking is that past performance can be an indicator of future performance. Often, with modest-sized accounts, a credit professional has little other than references on which to base a credit decision. Businesses applying for credit may know this and are unlikely to submit unfavorable references. Worse still, in the case of fraudulent operators, a potential creditor can simply invent their own references. In fact, 50 percent of all business credit frauds have fake references.

As with other fraud warning signs, it is important to recognize that most references are completely legitimate. However, there are certain questions that can be asked about the references being checked:

- Are the entities providing the references unknown?
- Do some or all of the references sound vaguely similar to known businesses?
- Do the references have an ostentatious sounding name?
- Are most of the references in the same general geographic area as the prospective customer?

If the answer to any of the questions is yes, further investigation is merited. The first and easiest step to take is to simply check the reference's locale. This small step may uncover many frauds. If the reference is found and the facts don't add up, a second step to help verify the legitimacy of references is to pull a credit report. Is the reference listed at all? If it is listed, is it in a line of business that makes sense? If not, and they are offering a glowing reference, it is a warning sign.

Another tip-off that a credit professional might be dealing with a questionable reference is the use of a mail drop or answering service. While a business that sells some product or service might operate from a mail drop, most businesses generally need a physical location.

The credit professional should be able to reach a reference. If they find that they are leaving messages at answering services, when a return call is received, the credit professional should say that they are momentarily tied up and state the need to call back. If the reference gives their answering service number again, the credit professional should ask for the number at the current location, as they will be calling in just a minute. Fraud operators hate to give their number, as they don't want their location known.

Often, fraud operators will stall indefinitely with a myriad of excuses as to why they will not be in their office and ask the credit professional to leave their number with the answering service. The excuses generally will sound plau-

sible, so good, common sense judgment is required. As with all situations, there are a number of legitimate reasons why a business person might want to give an answering service number. However, when this pattern of activity is seen and the references in question are overly glowing, the reports should be treated with more than a small amount of skepticism.

A post-mortem of credit frauds shows that many achieved success by relying on references that called back with glowing reports. A credit professional should still look for obvious discrepancies in the reference's story. If they have done their homework, and found that a reference does exist, does its story make sense in light of other information that they might have about the potential new customer? For example, is the reference reporting sales for longer than the new account appears to have been in business? Or is the figure given for high credit too high, in light of the size of the reference? If so, then the information received from the reference should be discounted and, perhaps, more questions asked.

One of the best indicators is a credit professional's instinct. When something feels wrong, a little extra investigation will usually dispel any qualms.



Comprehension Check

List four basic questions that can be asked about a credit reference to protect from business credit fraud.

Large Number of Reference Requests

Typically, clever bust-out artists establish a good credit history on a relatively smaller scale with several companies. They plan to use those companies as references when they begin placing larger orders. Often there is very little a credit professional can do to detect that this is a problem until the inquiries begin flooding in.

What constitutes a large number of inquiries? Most credit departments routinely receive credit reference requests; what is normal for one might not be normal for another. When something deviates from what is perceived as routine, it should be considered a red flag and more investigation is needed.

Often, there may be an explanation for the product or service ordered. Perhaps the inquiries relate to a major customer that is expanding. The best action for a credit professional to take is to simply call the customer and ask why they are giving their company as a reference so often. A legitimate company will be quite open and have a plausible explanation.

Bust-out artists are thoroughly prepared for questions about their ordering. Numerous companies that have established credit over a period of time used the excuse of expansion to justify huge increases in ordering from suppliers. A two-store chain is suddenly opening six more; or a wholesaler is suddenly going national. Stories may be similar, but if the company is not really known, it often pays to dig deeper.

If the customer claims to be opening new stores, has a sales representative visited the locations? What do the locations look like? Are they well stocked? Do they even have locations? Many companies claiming they were expanding were able to give only a vague explanation. It's the credit professional's job to pin down the buyer and ask for specifics. Why can't they give exact locations for their stores, if their new stores are the reason for increased orders?



Comprehension Check

Explain how an unusually large number of credit reference requests may indicate a possible business credit fraud.

Being the Credit Reference in a Possible Fraud

High inquiry rates also raise the question of what credit professionals should do when their company is used as a reference. Suppose many calls have been received and the credit experience has been quite good. What if the customer is fairly long term and has had substantially high credit and prompt payments? If the credit department is being flooded with inquiries, it may be a signal that fraud is in the making and liability may become a problem.

When companies begin to receive numerous inquiries about a particular customer, and then conclude that something is wrong, it is tempting to stop offering references altogether. Not responding to reference inquiries

reduces the valuable flow of information at a time when it is needed most. The credit professional should keep to the facts and leave interpretation to others; there is no reason not to offer credit references in a suspected fraud.

Increased Orders and Unusual Product Mixes

Increased Orders

The primary goal in any business endeavor is to get customers to increase their orders. But this can also be a warning sign of potential fraud.

In most credit fraud situations, the fraudster ultimately wants to order as much as possible. The window of opportunity for the heavy ordering is often just a few months. There comes a time in almost every credit fraud when ordering increases drastically because of greed. If they're going to take the business down, they can't resist doing it on a big scale. The results are orders that are out of proportion to the size of the business.

Like all fraud indicators, a credit analyst can only make use of this indicator in the context of other factors. Without knowing something about the business's history, its previous order history or its ability to move products, the credit analyst can't really make a judgment about whether a significant rise in orders is a warning sign. Here are some things to be aware of:

- If the order is from a retail store, what is the square footage?
- How many locations does the business have?
- Has a sales representative visited any of the stores or the headquarters? What did they find?
- If the customer is a wholesaler, is the reason for the increase known? Under normal circumstances, a wholesaler knows their sales team. If this is a mystery, try to find out who needs the product.
- Does the business have the usual signs of permanence?
- Are the backgrounds of the principals known?

When in doubt, a credit professional should ask their own sales team for help; a good sales representative can be one of the best fraud-fighting allies. If significant increases in ordering are being experienced, coupled with any of the other fraud warning signs, the odds are something is wrong.

When questioned after the fact, many fraud operators have told law enforcement agencies that an increase in ordering should be viewed by credit professionals as a red flag. Normal businesses do not routinely increase each order, but for bust-outs, this is par for the course. When a bust-out is gearing up, the orders generally increase each time.

Like all fraud warning signs, this may be merely a circumstantial red flag—something that should cause a careful look at the customer in question. Investigation should continue prior to authorizing increased credit.

Unusual Product Mixes

A classic indicator that a fraud may be in progress is the receipt of an order for an unusual product mix. This indicator usually comes in two forms. First, it can be a customer placing an order for a product that it wouldn't normally require (for example, a single restaurant ordering 12 copiers). Second, it can be a routine customer who places an order for a mix of product that does not seem to make sense (for example, six of every item).

Credit professionals should examine the first situation, regardless of the product or service sold, and develop a sense for the type of customer from whom orders are normally received. When an order is received that seemingly deviates from the norm, it generally stimulates that sixth sense. When this situation occurs, the game plan should always be the same; the normal credit investigation routine should be thrown out and the credit professional should become a detective. They should not stop until the reason for the odd order is understood. As with all fraud warning signs, it is important to keep in mind that many situations which look suspicious on the surface are easily explainable.

after further investigation. A conversation with the customer may alleviate fears of questionable activity or confirm original suspicions.

Another way in which this indicator can manifest itself is when the customer seems routine, but the order seems unusual. Generally, most credit professionals don't take the time to look at what is being ordered; the dollar value is what drives an investigation. The composition of the order is often a clue that the order is not valid. At trade shows, bust-out artists often place orders for each and every item in a company's catalog. Conversely, they might place an order for only one product, when normally an order would be a variety of items.

Through experience, this sense of which orders are unusual can be developed. Bust-outs have been detected by alert credit professionals who noticed that an order came in at a higher price than normal (retail, instead of wholesale, for example); an indicator that price is not a big concern. Be alert to the composition of orders. When in doubt, the investigation should continue until the reason for the order is understood.



Comprehension Check

Why can a sudden increase in orders or an unusual product mix be an indicator of a business credit fraud?

Misrepresentations

The question of whether something is a fraud ultimately rests on whether there is intent, and a misrepresentation of some sort generally proves intent. Therefore, anytime a misrepresentation is spotted, a warning flag should go up.

Anything can be misrepresented, including financial information, business or educational background, or reasons for a late payment. A credit professional may stumble onto a misrepresentation accidentally. Everything else about the potential account might look positive, causing the credit professional to ignore the one minor piece that points to something being amiss. Any misrepresentation, however small, is ignored at the peril of the creditor. While there may be occasional reasons to use an assumed name, it is a warning sign that more investigation is in order.

As with most fraud-spotting techniques, diligence and knowledge of the industry are the two elements needed to spot misrepresentations. The latter is critical because it sets off a red flag when something doesn't fit the norm for an industry. But even when there is no obvious sign of something wrong, diligence is really the key. When it comes to the **Five Cs of Credit**, the C for character is the most important of all. Evidence of a misrepresentation is critical in an analysis of a person's character.

Undisclosed Changes in Ownership

Changes in ownership occur every day, and the vast majority are completely legitimate. However, there are many individuals who specialize in buying businesses with the sole intention of driving them into insolvency, keeping the assets for themselves and leaving creditors unpaid. This form of business credit fraud causes greater losses than all other forms put together.

There are several key warning signs that signal questionable ownership changes. One warning sign is a new owner with a track record of bankrupting businesses. Unfortunately, most are not so obvious. A second warning sign is an ownership change with little or no notice given to creditors. In most instances, suppliers (trade creditors) and others associated with the business are notified of an ownership change. But credit fraud operators often like to capitalize on the good name of the business, and downplay the new ownership.

Another indication that something might be wrong is a new owner with little or no background information available. Often, fraud operators, also called take-down artists, take over businesses through fronts. The real owner, or take-down operator, has such a bad track record that their name cannot appear on a business without raising suspicions. The object is to find a clean front man. In this case, there may be a new owner of a business whose prior business experience seems insufficient to have provided either the capital or the experience to purchase and operate the business in question.

Another warning sign is when a company is owned by a series of corporations, and a trace up the corporate ladder only seems to reach more parent companies—no actual people. After all, people run a business and a business

is only as good as the people running it. If it's impossible to identify who is in charge, it may be an indication that something is being hidden purposefully when transparency in business conduct is so important.

The credit professional should work upstream in an attempt to determine the owners of the ultimate top parent. If it's been specifically advised that the names of the owners are not going to be released, this is clearly a warning sign.

Unverifiable Backgrounds of Principals

Perhaps the most important criteria in the evaluation of the creditworthiness of a business is the background of the principals. If someone has a long and verifiable track record, a credit analyst can feel comfortable that a successful past will likely be a prologue to a good future.

When studying a business for the extension of credit, it is a best practice to pay particular attention to the antecedents of the principals. Experience and criminology studies have shown that white-collar criminals will continue their schemes until caught. After the first bust-out, fraud operators have several choices: (1) they can tell credit agencies and creditors the truth, in which case, credit likely will be withheld; (2) they can make up a background; or (3) they can simply defer it.

The first scenario isn't likely, but it does occur. Some debtors are upfront about their past problems and attempt to convince creditors that they have turned over a new leaf. While this works occasionally, the second or third options are more likely scenarios.

Bust-out operators will sometimes supply credit agencies with personal background information which, for whatever reason, cannot be verified. They do this by saying they worked for firms which are now bankrupt or which never existed. Access to online information and credit reports has gone a long way toward closing the information gap.

Dealing with an Unverifiable Background

When in possession of a large order, the credit professional should ask questions until comfortable with the principal's background. The key is to ask for specific addresses of previous employers. Once this information has been obtained, it is easier to verify the background. Another method is to ask for the principal's supervisor at a particular company. If the person is reluctant to supply this information, it should be a clear red flag for the prospective creditor.

Hidden Ownership

As already stated, the most important C of the **Five Cs of Credit** is character: knowing all about the owners of customer companies is critical to good credit analysis. While there may be some legitimate reasons why someone would want to conceal their ownership of a business (such as being a publicity shy celebrity), in most instances, it should be a warning sign to the credit analyst. There are two questions: how can a business operate with a hidden owner and, assuming they are hidden, what then?

The first situation is more common than one might think. Because the second question is tougher, hidden ownership most often occurs after an ownership change, meaning that control changes should be monitored very carefully. Whether there are new owners or not, here are a few warning signs:

1. **Reluctance of the listed principals, or managers, to make decisions without consulting someone else** is a clue that it could be a front. Generally speaking, when dealing with an owner of a business, they are able to answer routine questions. However, if someone is merely a front for a hidden owner, they will be unable to answer questions without first checking with the real owner.
2. **A control change where the owners are not immediately disclosed.** Most ownership changes are not kept secret; if they occur with little or no fanfare, the individuals who are

represented as principals need to be checked to see if they have backgrounds commensurate with their new positions.

3. **A confusing chain of command at a company.** Ask company representatives at suspect businesses for the names and titles of the principals at the company. If they respond that someone is simply the boss when they are not the highest-ranking principal, it is possible that something is amiss.
4. **A confusing corporate structure.** While it is possible that a corporation takes over a long-time customer, it is important to find out who owns the corporation. Sometimes, individuals with checkered backgrounds hide behind a series of corporations. This tactic also makes it harder for the eventual lawsuits to reach them. In cases where there is a series of corporations going up the ladder, each with unknown principals, a credit analysis should not continue until the actual people with titles and responsibilities are reached. This sometimes happens legitimately, of course, but it is also a method used by con artists to remain hidden from the scrutiny of creditors and regulators.
5. **Signers on checking accounts.** An old adage in white-collar crime investigations is “follow the money.” If a situation is questionable, and the real owners may not be known, the credit professional should try to determine who the signers on checking accounts are. When it is found that the signers are different than the purported owners, it clearly raises the question as to why someone other than the owner has control of the funds.

Sources of Information

While it is possible to find out about hidden ownership on one’s own, it is often very difficult, and simply happens by accident on many occasions.

Key areas that provide help:

1. **The sales force.** Some of the best leads may come from credit professionals who paid attention to what their sales departments tells them. Keeping open lines of communication with sales is one of the best ways to gather useful information about the customer base.
2. **Industry credit groups.** Industry credit groups are an invaluable source of information about ownership changes and irregularities.

Principal Unavailable

The unavailability of a principal over a period of time may signal that an operation is winding down. There are also many instances where fraudulent debtors are unavailable at the time of ordering. Frequently, this occurs with operations that place orders for delivery to mail receiving agencies or mini-storage warehouses. Because “the customer is always right,” it is possible to overlook warning signals and to fill orders even from blatantly questionable operations. If customers are difficult to reach to discuss an order, the odds of reaching them after a shipment or to collect a past due only decreases. Some of the classic excuses by fraudulent debtors include:

- He’s in the field, collecting from our customers. It’s hard to fault someone who’s out trying to shore up cash flow; most credit professionals can relate to this excuse.
- She’s overseas, on a buying trip. While this may be what creditors’ hear, there is often no basis in reality for such statements.
- He’s had a heart attack. White-collar criminals are known to have multiple heart attacks when creditors are trying to reach them to discuss delinquency issues.

- A principal may be unavailable because the person listed on paper as the principal may, in fact, be a front for another. In such a case, it will be unlikely the listed principal will deal with the creditor on matters of substance.

Any of these scenarios should raise a red flag for the credit professional. Most importantly, the unavailable principal is a clue that can help define the nature of the transaction.



Comprehension Check

Describe why a change in ownership, unverifiable background of principals, hidden ownership and unavailable principals need further investigation and may be warning signs of fraud.

NSF Checks Received

Like virtually all potential signs of fraud, NSF (non-sufficient funds) checks should only be taken in the overall context of the business. The NSF check is simply one more indication that something may be amiss. The key in determining fraud is state of mind and intent. Most of the time, an NSF check simply reflects poor management or a miscalculation and may not reflect a fraud. However, when dealing with a fraud, a bounced check is probably intentional. Some factors to consider are:

1. **Patterns of activity.** While not generally admissible in court, patterns can serve as strong circumstantial evidence that something is amiss. NSF checks can be an indication that something more than poor management is involved.
2. **Fraud audits conducted after the fact often uncover other NSF checks going into a fraudster's checking account.** The checks are often submitted from related parties just prior to the issuance of a flurry of NSF checks. The perpetrator can then claim that money was in the account, and show deposit slips to prove intentions were good.
3. **An increase in ordering at the time an NSF check is submitted.** An NSF check that precedes a large order could serve as a tipoff that a fraud may be in the making.

An NSF check is not necessarily an indication of a fraud. But looked at in connection with other information, it can be one more clue of a potential fraud, rather than a routine business transaction.

Counterfeit Checks Received

Check fraud is a challenge given the advent of inexpensive desktop publishing systems, laser printers and color copiers, an individual con man can manufacture checks quite easily.

The following tips may help spot forgeries and save costly errors in trusting too much in appearances. Part of the trick in catching check forgeries is to focus special attention on those accounts that appear suspect. The warning signs to look for when a bad check is suspected:

- Check numbers do not change.
- Checks drawn on new accounts.
- Checks with no account or routing number.
- Inverted watermark on paper.
- Misspelled words.
- Poor printing quality.
- Checks presented near the end of the business day by customers who seem unwilling to wait until the next business day for their order.
- Checks received from customers whose accounts are themselves suspect.
- Normal checks presented to honor a previously submitted bad check.

- Irregular signatures, such as those with an interruption or gap where the pen has lifted off the paper completely.
- First four digits of routing code are not valid.
- District in routing code does not match District in transit number.
- Bank identification number in routing code does not match bank identification number in transit code.
- Check identification in optical scan numbers at bottom of check does not match check number on face of the check.



Comprehension Check

List some warning signs of a bad check.

Financial Statement Irregularities

One of the best ways to uncover potential frauds is through the careful analysis of a business's financial statements. It is not necessary to be a CPA; all that is needed is a working knowledge of the basics along with an eye for detail.

Financial statement analysis gets to the core of the **Five Cs of Credit**. Statements are used to determine whether the capital and collateral of a business are sufficient to extend credit. Unless the character of the maker of the financial statements is totally sound, the analysis will be based on faulty information. There have been countless decisions wrongly made because they were based on phony information.

Context is critical in helping a credit professional determine that a financial statement has been fabricated or doctored. Statements should always be examined in the context of all other information known about a business. A financial statement is designed to paint a picture of a business both at a given point in time (through the balance sheet), and of its progress over time (the income statement/statement of activities). Both statements should make sense in light of other information that exists about the business. In the context of other information, each piece should fit together; misrepresentations often do not fit. This is where knowledge of a particular industry and the economy will help identify a financial statement that may not be fully reflective of a business's true picture.

Often, credit professionals and investment professionals are taken completely by surprise by the bankruptcy of a company that appeared, based on years of audited statements, to be making money. W. T. Grant's notable bankruptcy in the early '70s is a great example of a surprise bankruptcy, which, in retrospect, offered clues in its financial statements that it was destined for failure. Unfortunately, those taken by surprise suffered their greatest losses as a result.

W.T. Grant, one of the largest retailers in the country, had shown good income numbers over the years leading up to its sudden bankruptcy. While it did pay slowly, creditors felt comfortable that the risks were reasonable, given the fact that W.T. Grant was an old-line, profitable account. The missed clue in the financial statement was severely negative cash flow.

It is important to keep in mind that generally accepted accounting principles (GAAP) allow businesses wide latitude in accounting policies. Those with very aggressive policies may often overstate the soundness of their financial status. W.T. Grant's negative cash flows gave significant advance warning, but its income statement did not. It made money only based on highly aggressive policies, which were within GAAP until it declared bankruptcy.

Assets Removed

Assets removed are the essence of any business credit fraud. While bust-outs are often thought of in terms of the removal of inventory, a business is made up of far more assets than inventory, and any asset of a business is subject to looting. Generally, the removal of assets is not noticed until it is too late, but in some instances, a credit or finance professional can spot this early, before the damage is too severe.

In an effort to show intent, one question to ask is, does the removal of assets occur to such a degree that keeping the business afloat is impossible? In many instances, the rapid speed and huge quantity of assets removed make it

obvious to any creditor that a business was being pillaged solely for the purposes of enriching its owner, and there was no intent to keep it a going enterprise, and pay creditors.

What may seem obvious to professionals may not be obvious in a court of law. It is difficult to determine malintent when studying the removal of assets. Even if too much of a business's assets are removed, showing intent can be challenging. Legitimate businesses fail every day, and the owners continue to draw salaries right up to the end.

One way to show intent, in the case of removal of assets, is a misrepresentation. One example is the case of Coats Distributors, a business purchased by convicted bust-out operator, Jon Miller. Miller claimed to be infusing money into the business. He actually transferred hundreds of thousand dollars into Coats. However, investigators found that it was only a partial return of an even greater amount that he had already removed from Coats' operating accounts. On a net basis, Miller had removed more than \$400,000 almost immediately after gaining control of the business while, at the same time, purporting to be infusing cash into the business. This appears obvious, but at the time, credit, financial and law enforcement investigators didn't have the benefit of seeing the whole picture. They only had the word of Jon Miller to believe.

Any Asset Can Be Removed

Asset removal is not only limited to inventory or operating cash. Corporate pirates will take anything of value. Look at any balance sheet; there are all kinds of items of value. One of the biggest is, of course, accounts receivable; they simply can be collected and pocketed, or they can be sold or factored to a third party. Many fraudsters, when factoring their accounts receivable, supplement the real receivables with phony receivables.

Even harder assets, such as equipment or real estate, can be converted to the owner's use, through sales or sale-leaseback arrangements.

Despite the difficulty of proving intent, credit and finance professionals should always keep a lookout for a business removing assets at a fast pace. It can be more than mismanagement. The removal of assets can be at once the most obvious or the subtlest of all the fraud warning signs.



Comprehension Check

Why is it important to keep an eye on a customer's assets and make sure they are not improperly removed?

Identity Theft and Social Engineering

Business identity fraudsters do not need to steal much of the information needed to impersonate a business; more often than not it is publicly available at no cost or legally purchased. In most states, businesses are required by law to post documents that contain many of their key identifiers such as sales tax number, business license number, etc. Unlike the protections provided for consumer credit reports, if a business has a credit report, virtually anyone can order a copy because business credit reports are intended to foster and promote commerce. Unfortunately, business credit reports contain a wealth of information that can also be misused by crafty business identity thieves.

Business EINs

In some respects, an **EIN**, a *business' federal employer identification number*, is a business form of a Social Security number because of the ways it is commonly used to uniquely identify the business. An EIN is not provided the same protections as an SSN. Many business identity theft schemes occur, and many fraudulent accounts can be opened, with only a business's name, address and EIN. State business registration information is public record showing details about the business's legal structure, ownership, officers, directors, registered agent and registered address. In some cases, copies of documents that contain the owners' or officers' signatures are legally available to anyone who is ambitious enough to look. Of course, there is the Internet black market where the stolen confidential information of millions of consumers and businesses is routinely purchased, sold and traded every day. Fueled by wide-scale data breaches caused by hacking, theft, loss, or human error, there are countless consumer and business credit card numbers, account numbers and other sensitive information available for the taking.



Comprehension Check

Explain how EINs make identity theft easier.

Corporate Identity Theft

Identity theft and social engineering are among payment scams that are neither new nor particularly complicated. Fraud perpetrators target companies in what they believe are routine, business-to-business transactions. Bad actors pretend to be a company, with just enough information through social engineering to get funds wired to their account.

Criminals impersonating legitimate business owners or businesses have gotten ever more sophisticated as public attention to their chosen, illegal profession has increased. With the Internet making company information readily accessible, many potential fraudsters can easily copy company logos, letterheads or other paperwork from a company's website to make their communications with targeted businesses seem less suspicious. Still, these applications often contain a number of red flags in their details and operational history. Credit professionals can save their company from losses with thorough investigation.

The key to detecting a fraudster using a legitimate company to place orders is to take a hard look at the actual applications and orders, which often have errors on them, (e.g., misspellings, etc.). Credit professionals should take the time to compare the information provided on an application with the information included in a company's report to reveal the potential buyer's identity. Take advantage of the resources available such as an NACM National Trade Credit Report to verify the information provided and check the inquiry rate on the NACM report. Contact and shipping information should also sound alarms for credit professionals aiming to ensure that their potential sale is legitimate. Fraudsters often ship to residences and mailbox locations which may be detected by conducting a reverse look up on the shipping address. Examine the email address carefully; a lot of fraud is coming from legitimate_company@yahoo, Hotmail, Gmail and other free, untraceable email addresses. Beware of email addresses and phone numbers that are slightly different than those of the verified legitimate company.

Many companies and credit professionals may think that the longer a company has been in business, the less of a risk it is to sell to them. But an application or report that shows a company has been incorporated for several years doesn't guarantee that the buyer is legitimate. Sometimes the fraudsters will establish a company, or incorporate four or five companies, and let them become dormant. These shell companies will often be inactive as they rack up the number of years incorporated and then suddenly see a flurry of activity. While this doesn't automatically indicate the presence of fraud, a potential customer who has been dormant for a long time and suddenly begins seeking credit should be investigated further.

Fraud on the Rise

Many domestic companies were affected by payment fraud in recent years. Federal Trade Commission research shows that, of 30 types of fraud complaints, the top three are identity theft, debt collection schemes and imposter scams, which together accounted for more than one-third of all reported incidents. Businesses with otherwise sterling reputations are finding themselves fielding complaints, some of which end up with the Better Business Bureau or Attorneys General offices in various states. Once the business customer clicks on an email link, often to accounts through Gmail or Outlook rather than a company's ".com" or ".org" domain, or takes a phone call and provides information without checking the source, the process of fraud is off and running. Despite all the warnings about scams over the years, such schemes continue to be alarmingly successful.

Whether it's a bust out, where either a criminal or a shell company set up by the criminal will buy goods without ever intending to pay for them; or corporate identity theft, where a criminal pretends to be from another legitimate business and submits an application for credit; another online scam or another form of cybercrime, thieves will exploit the weakness of an industry, an owner, or a company to get what they're after. Moreover, by seeking certain amounts according to certain business conditions and characteristics, these thieves can also keep themselves from getting caught. Depending on the size of the company, a fraudster or identity thief might seek \$5,000, \$10,000, \$25,000 or even up to \$100,000 worth of credit, or a commensurate amount of goods. If a company usually writes off a certain percentage of bad debt, and is expecting to write more off during the recession, a criminal can often put in the application, get it approved quickly and then never even face a cursory investigation by the company itself.

All of these instances add up. Business identity theft currently costs companies \$50 billion a year in the U.S., and this isn't just a problem for large firms. Certain industries face greater threats due to the resalable nature of their products, like electronics, computers, technology and even food, but identity thieves find small businesses just as profitable as large ones. No matter the business situation, identity theft is a sizeable and costly problem that requires diligence on the part of company credit staff to make sure the person or company asking for money or goods is who they say they are.

Bust-Out King Reveals Secrets to a Successful Scam*

Three years after his release from prison, Al Forman is a grateful man. Speaking at symposium in Las Vegas in 1994, he thanked credit managers, investigators and even the FBI agent who ultimately arrested him.

These people brought down one of the most successful bust-out artists ever and Forman credits them with helping him straighten out his life and enabling him to make strides in the art of living.

Standing at a podium facing a crowd of more than 100 credit managers and financial professionals from around the country, Forman began his foray into public speaking fumbling with index cards and telling his life story before finally getting down to what everyone was gathered to hear: how he did it.

What Al Forman did fooled creditors and investigators for a decade while setting up and deliberately bankrupting numerous companies. He was involved in more than 20 different businesses during this time and, at his peak, had four separate bust-outs operating simultaneously.

Forman, who was 54 at the time, admits he has no idea where the term bust-out originated, but he certainly understands its meaning. A bust-out is a planned bankruptcy or insolvency, often of a phony company that sells merchandise from other companies. By first placing small orders with suppliers, the bust-out artist gradually gains the trust of creditors and eventually works up to larger orders. By selling the products at discounts of 25 percent or more, the bust-out artist can pay for smaller orders until the time is right for the bust-out. Because creditors do not expect payment for 30 to 90 days, the bust-out artist can order and receive bulk shipments without paying right away. And when creditors finally do run out of patience, the bust-out artist files for bankruptcy or disappears.

From the early 1970s until his arrest in 1985, Forman mastered the bust-out. In all, his crimes cost creditors about \$40 million, averaging \$1 to \$4 million per bust-out. At the time of his arrest, he was managing bust-outs in Pittsburgh, Rochester, Long Island and Ft. Lauderdale. By Thanksgiving of 1985, all four operations were in high gear with products coming in by the trailer load.

"All things have a beginning and an end," Forman said. "I really do believe that if I wasn't caught, those four bust-outs were going to be my last."

With creditors, FBI investigators and the U.S. Postal Service trailing him, Forman was finally arrested and convicted of mail fraud and interstate transportation of stolen property and sentenced to 17 years in prison. He served six years and was released in 1991.

How He Did It

According to Forman, there are six necessary components to a good bust-out:

1. Capital, preferably \$100,000 or more;
2. A capable front man;
3. Good location from which to receive and ship merchandise;
4. Equipment;
5. Financial statement; and
6. A corporation.

Once these elements were in place, 99 percent of suppliers that Forman contacted shipped to his phony companies without a thought and were defrauded. In addition to the six elements above, Forman found that it is unwise to place too many orders at trade shows, because all orders are checked by a credit reporting agency. He made sure that a front man attending a trade show never placed more than six orders.

By adhering to a few basic rules and lining up the six elements, everything just fell into place—creditors approved orders, merchandise was shipped without payment, and the bust-out company in turn sold at discount to retailers and suppliers. Creditors readily increased credit lines and Forman was surprised at how easy it was to go from a \$3,000 limit to more than \$10,000.

“A good bust-out is an illusion where you paint a picture that I’m going to buy your merchandise and sell your merchandise. But I’m not going to pay the bills,” he said. “There isn’t a salesperson around who doesn’t like large orders.”

The Fall

After a long run of successful bust-outs, investigators began asking questions. Forman was questioned by the FBI in Boston about a company that had filed for bankruptcy. That deal had started with Forman’s father-in-law and Forman was one of the company’s clients. After that, more questions arose and Forman was followed by FBI agents. A few days before Christmas in 1985, all of the warehouses were closed and Forman and his father-in-law were arrested.

“All I could think about was that famous expression, ‘I woulda, coulda, shoulda.’”

Although Forman expresses remorse for his crimes, and served time in prison, credit and financial professionals were not satisfied.

“I’m very surprised that his sentence was so light and that he’s out right now and gainfully employed talking about it,” said a credit manager from Procter & Gamble, Cincinnati. “He should probably still be [in jail] or at least making some restitution and that didn’t come through in his speech at all.”

A credit manager from Ralston Purina, St. Louis, agreed, explaining, “After many years of seeing his name, it was interesting to see him face to face. But I agree that he probably shouldn’t be out.”

Forman served six years in prison for his crimes. Many would say that isn’t enough, but compared with many other white collar crime offenders (Michael Milken and Ivan Boesky served less time), that is a substantial amount of time.

Practices like Forman’s bust-outs are not uncommon today and the problem of fraud in American business is growing.

With law enforcement concentrating on problems like drugs and violent crime, fraud is increasing. Law enforcement’s resources are limited in its fight against white collar crime and private industry must institute internal and external controls to protect itself from fraud.

Forman’s Future

After all that Forman learned during his decade-long bust-out spree, perhaps no lesson proved more profound than that of getting caught. He went on to work in the health food industry and began lecturing on his experiences. But Forman insists that creditors will not have to worry about any future problems from him.

“I have done harm for what at the time seemed to be good motives,” Forman said. “Sometimes my supposed love of others was in reality only a desire to dominate them. Looking back, I wish I had learned to master myself, to control my impulses, and curb my cravings for power, possessions, and pleasure. What has happened to my life’s progress the last three years, I’ve made strides in the art of living so that what I admire in people, others can admire in me. Perhaps a little, but certainly not enough.”

**Reprinted from NACM’s Business Credit magazine, January 1995. Originally written by Kevin C. Naff, former communications associate editor.*

Key Terms and Concepts.....



Assets removed, 12-10–12-11	Increased orders, 12-5
Bust-out fraud (sleeper fraud), 12-2, 12-14–12-20	Industry credit groups, 12-8
Changes in ownership, 12-6–12-7	Large number of references, 12-4
Corporate identity theft, 12-12	Misrepresentations, 12-6
Counterfeit checks, 12-9–12-10	NSF checks, 12-9
Credit references, 12-4–12-5	Principals unavailable, 12-8–12-9
EIN (employer identification number), 12-11	Product mixes, unusual, 12-5–12-6
Financial statements, irregularities, 12-10	Sales force, 12-8
Five Cs of Credit, 12-6, 12-7, 12-10	Same name scam, 12-2
Fraud, 12-2	Unsolicited orders, 12-3
Hidden ownership, 12-7–12-8	Unverifiable backgrounds of principals, 12-7
Identity theft, 12-11–12-12	Unverifiable references, 12-3–12-4

Comprehension Check.....



1. List four basic questions that can be asked about a credit reference to protect from business credit fraud.
2. Explain how an unusually large number of credit reference requests may indicate a possible business credit fraud.
3. Why can a sudden increase in orders or an unusual product mix be an indicator of a business credit fraud?
4. Describe why a change in ownership, unverifiable background of principals, hidden ownership and unavailable principals need further investigation and may be warning signs of fraud.
5. List some warning signs of a bad check.
6. Why is it important to keep an eye on a customer's assets and make sure they are not improperly removed?
7. Explain how **EINs** make identity theft easier.

Summary.....



- Business fraud costs businesses billions of dollars every year. It is critical for a credit professional to be aware of business practices that may seem out of the ordinary.
- Fraud takes a variety of forms, but is normally done through the intentional manipulation of the truth in order to do harm to another party. Common techniques used to commit fraud include:
 - **Bust-out scams**
 - **Same name scams**
 - **Unsolicited orders**
 - **Unverifiable references**

- Large number of reference requests
 - Increased orders or unusual product mixes
 - Undisclosed changes in ownership
 - Unverifiable backgrounds of principles
 - Hidden ownership
 - Financial statement irregularities
 - Identity theft
- There are often very reasonable explanations for irregularities in business operations. However, it is very important that, if a credit professional believes something is out of the ordinary, a credit investigation be conducted. This can be as simple as calling the customer in order to prompt an explanation. If a company applying for credit seems to be holding back information that should be readily available, or a principal is avoiding inquiries at all costs, they may be stalling in order to commit fraud.
 - The best sources of information for a credit professional who suspects fraud are the sales force and industry credit groups.
 - Due to a creditor's need for the free flow of information, businesses are often not afforded the same protection as individuals. Credit reports and business EINs may make it easy for a thief to steal a business's identity. Over 30 types of fraud have been identified with the top three complaints being identity theft, debt collections schemes and imposter scams. It is critical that a credit professional be aware of these scams and remember that, "If it seems too good to be true, it probably is."

References and Resources



Business Credit. Columbia, MD: National Association of Credit Management. (This 9 issues/year publication is a continuous source of relevant articles and information. Archived articles from *Business Credit* magazine are available through the web-based NACM Resource Library, which is a benefit of NACM membership.)

Carr, Matthew. "Attack of the Doppelgangers: A Case Study." *Business Credit*. Columbia, MD. National Association of Credit Management. June 2008.

Naff, Kevin. "Bust-out King Reveals Secrets to a Successful Scam." *Business Credit*. Columbia, MD. National Association of Credit Management. January 1995.

Office of the Attorney General of Florida, Consumer Protection. <http://myfloridalegal.com/consumer>.

U.S. Department of Justice, Criminal Division/Fraud Section. www.usdoj.gov/criminal/fraud.

Supplementary Material

Attack of the Doppelgangers: A Case Study*

WESCO Distribution

In 1922, Westinghouse Electric Company created WESCO to sell and distribute its growing catalog of products. The organization flourished and in 1994, the management team of WESCO, in partnership with the private investment company Clayton, Dubilier & Rice, purchased WESCO from Westinghouse. The holding company WESCO International was formed following another purchase in 1998, and the following year the company went public on the New York Stock Exchange. It is a Fortune 500 success with more than \$5 billion in annual sales, 7,000 employees in 400 full-service centers and over 110,000 customers around the globe.

But in July 2006, an individual claiming to be the manager of WESCO's Cleveland, Ohio branch began placing purchase orders with several computer distributors for seemingly innocuous items such as toner, ink cartridges and computer memory sticks. The distributors took the orders and began sending invoices to the Cleveland branch, which then forwarded them on to corporate.

"That's basically how it started," said William Coe, asset protection manager, WESCO. "We initially thought, as I started the investigation, that it was an isolated incident; that somebody was impersonating this branch manager in the Cleveland area. I had no idea that it had far-reaching implications into international areas."

Shortly after, a similar situation came to light as someone posing as WESCO's chief executive officer (CEO) began submitting orders for the same items. They'd place an order for several thousand dollars and ask for a line of credit. Almost all of the transactions took place over the Internet and the salesmen for the distributors failed to place a single phone call to verify any of the information or authority. The emails from the individual claiming to be WESCO's CEO and others arrogantly provided a series of phone numbers, knowing that if any of these would have been dialed, they would have been found out to be fictitious or disconnected.

In trying to convince law enforcement to take up the case, WESCO found itself in a strange situation as it wasn't a victim in the classic sense; the company wasn't suffering a loss. It was the network of suppliers and customers that WESCO did business with that were targeted and faced the loss of tens of thousands of dollars.

"I guess the sad thing about this is, legally, we're not out any money," stated Coe. "The biggest problem we had was that because we are publicly traded, our reputation was at stake. We could ill-afford to have the Wall Street analysts or others start bad-mouthing WESCO for being mixed up in some type of scam. That's one of the reasons why we started collecting all this data and contacting the U.S. Secret Service once we found out it was a large operation that was organized and targeting hundreds of companies. They targeted everything from Dells to HPs down to the mom-and-pops running out of their garage."

Simplicity and Villainy

Between July 2006 and the end of 2007, fraudsters parading as WESCO representatives hit at least 1,500 companies. The assault didn't slow as another 200 companies contacted WESCO in the first quarter of 2008, reporting they had received fraudulent purchase orders in the company's name. The approach the scammers used is simple, yet elegant. It also clearly demonstrates that, even though there are countless warnings about email scams, there is still a broad naïve base out there for criminals to readily and successfully prey upon.

The perpetrators would pose as anything from a corporate executive at WESCO, to a purchasing agent, to one of the company's 400 branch managers. The vast majority of the contact was done via email, originating from addresses that have WESCO somewhere in the name. Coe has identified more than 40 different email addresses and at least two dozen different individuals for whom the scammers have posed. In some cases it would be a genuine person, like the CEO, CFO or a number of other executives, or it would be a common name plucked from the air that by chance would match with someone from WESCO's large employee base.

"We have an Internet site of wescodist.com. The fraudsters would use wescodistr.com or they might have wescodists.com or wescocompany.com," explained Coe. "It's just a little variation. Then it started appearing as the

first part of the address, like wescosales@earthlink.net or wescoppm@gmail.com. So, they started using all sorts of free email providers like Yahoo! and EarthLink.”

Even more devious was that the perpetrators also began contacting distributors using TTY/TDD telephones for the hearing impaired. The service is toll-free and uses an operator to relay responses between a hearing impaired person and another party by reading aloud what was typed by the hearing impaired individual and then by typing what was said by the other party. This allowed the perpetrators to hide their voices.

The basic scenario consists of the fraudsters asking for a quote on first contact, and once that was received, they would come back with a purchase order. The purchase order, a fairly uniform document, would be legitimate looking enough, including a WESCO logo that had been extracted from one of the company’s websites and placed in the letterhead to make it look more official. When the fraudulent purchase order was sent, it was typically for between \$30,000 and \$60,000 and they would ask for net 30 terms. On a few occasions, multiple credit cards were used to pay for the order, but most of the time they were given a line of credit. If a credit application was sent to be filled out, the information was readily available. Since WESCO is a publicly traded company, the pertinent information could be gathered through one of the company’s websites or through its prospectus.

“They tried to target salesmen versus management ... to dangle that nice commission for that guy out there,” said Coe. “Once they got that initial purchase, it would quickly be followed by several other purchases of equal or greater value, but it would be the same type of items, almost identical. They would try to instill a sense of urgency by insisting that they needed the items yesterday and needed them shipped overnight to a particular address. Basically, they didn’t care how much it would cost for them to ship it.” Coe added, “They were counting on a degree of greed from the commissioned sales person and then they were also counting on this sense of urgency to keep those sales people from practicing due diligence.”

To add to the convincing scheme, the fraudsters were armed with WESCO’s Dun & Bradstreet number, which is also readily available, as well as some of WESCO’s references. “The problem is some of the suppliers dealing with us on a regular basis would naturally send the products out,” stated Coe. “They would not question it because we had already established lines of credit.” Unfortunately, the lack of follow-through has cost some of the duped companies as much as \$750,000, the result of a single salesman who hurriedly sent out product in anticipation of a big commission.

As usual, there were plenty of warning signs, but they were simply ignored. As Coe related, “The dollar tends to blind individuals to some of these obvious red flags.” For example, after making an order, the fraudsters would provide a point of contact which was usually a residential address somewhere in the United States. And in every single case, the address was different than where the person making the call was supposedly located.

The sad truth is that the individuals that lived in the homes that these items were being shipped to were victims themselves. In some cases, they had met the criminals online in a chat room or some other virtual venue and had fallen in love with them. The fraudsters said that they needed a favor, and the love-struck individuals readily accepted. The perpetrators found others by trolling job search sites, and, knowing these people were in need of work, asked if they would like a position with WESCO as a “freight forwarder.” The job was easy enough: the individuals could work from home accepting deliveries and all they had to do was re-label the boxes to have them shipped outside of the country. The fraudsters even got these people to pay for the overseas shipping charges out of their own pockets with the promise that any money they spent would be reimbursed. A little while back, WESCO had a series of checks sent out to suppliers stolen in transit. These were reproduced in a variety of different forms, and even sent as paychecks, just like a regular WESCO employee, to these duped “freight forwarders.” Unfortunately, 10 to 12 days later, the bank would come back and inform them that the check was fictitious. But by then it was too late, the fraudsters had gotten to use these individuals and their homes for close to 40 days, with shipments arriving and being sent overnight. They had already moved on to their next victim.

“There were no arrests of these people because they were basically unaware of what they were doing,” recounted Coe. The freight forwarders shipped the boxes to a legitimate importer/exporter in the United Kingdom, who then forwarded them on to Nigeria. From Nigeria, many items like toner and ink cartridges don’t have serial numbers and are readily disposable. They then make their way back into the U.S. via Canada and Mexico and are reportedly sold at discount outlets. Computer supplies and peripherals aren’t the only items to have been targeted.

Larger ticket items like earth-moving equipment from Caterpillar, diesel engines and diesel engine parts and LCD projectors have also been scammed.

Even WESCO itself has been a victim. A company that WESCO purchased was contacted by the fraudsters with the standard script. In an act of overzealousness, and wanting to show the new parent company that they could ship with the best of them, this newly acquired company shipped over \$100,000 worth of product to the criminals. Fortunately, this worked to WESCO's advantage, to a degree. Since the company had all the tracking information, the Secret Service was able to trace the merchandise to locations in Washington State and Florida, where it had been forwarded to London. In London, the Secret Service had a detachment that went to the importer/exporter and located some of the boxes. Others had already been sent on to Nigeria. A short time after that, the Secret Service made two arrests of Nigerian nationals and confiscated tens of thousands of dollars worth of merchandise. The two men were incarcerated in Nigeria, as extradition to the United States is a tangled and complicated process.

Even more frustrating than its name being blighted said Coe is that WESCO has now become a mark. "The thing that I am more concerned about than anything else, and we've found this in the past couple weeks, is that we're seeing evidence that the fraudsters are impersonating other large companies and using their identities to target WESCO," explained Coe. "We've put out several fraud alerts to our people because I knew the other shoe was going to drop; it was just a matter of time before we would be a target."

Lessons Learned

The WESCO case, which is just one of a seemingly growing number, shows that there has to be greater due diligence on the part of everyone and, most importantly, sales staff. The Federal Trade Commission and the U.S. Secret Service do not keep statistics on how many companies are affected each year by these attacks, or how much money is ultimately lost. WESCO alone has had nearly 2,000 companies report receiving fraudulent purchase orders in its name. The company made a bold move by posting a security caution on its website informing any company that has even the slightest suspicion about an order to contact the company directly via telephone.

"I think that in putting something like that on our website shows we are concerned, not only about our business and our reputation, but also in trying to protect the public and our fellow distributors," said Coe.

The larger issue is how easily the fraudsters are able to perpetrate these scams and often how easily some individuals are fooled. "I could register www.cocacolacorp.com today, create a fake website and offer you a free case of Coke if you go to my website and give me personal information," said Tzanis. "I am sure it happens everyday via spam emails. But I doubt that spammers are specifically targeting companies that often. They will take what they can get."

Tzanis relayed information easily obtained from a public website that provided instructions on how to "spoof" emails and pose as an employee of a company. It also demonstrated how shockingly simple it was to perpetrate with even modest computer skills. "In the WESCO case, that person could have actually used the president's email address to send those 'spoofing' orders," explained Tzanis.

The onus is on all staff members to be vigilant.

"You really can't prevent this from happening. The only thing you can do is the security caution, which we did eventually," Coe said. When your company is a publicly traded Fortune 500, your company's information is out there, you can't prevent that and you can't prevent ID theft. "It's almost impossible," Coe said. "And it's not until you start getting the invoices or you start getting queries from third parties do you know that it's even occurring."

Legally, it's a difficult situation when a company's name is being used to defraud others. Enforcement often-times builds a case on substantiated loss. WESCO had to convince the Secret Service that the fraud posed a potential loss of reputation, which could be even more damaging in the long run. "Reputational damage is long-lasting," stated Coe. "Thousands of dollars in a loss is nothing versus the millions lost in a downtick of stock prices that can decimate a company."

Credit and sales staff have a variety of tools available to them. If an email with a suspicious originating web address is received, a simple search on registration sites like GoDaddy.com or a "Who Is" search on NetworkSolutions.com will tell when a web address was registered, who the administrator is and where they're located. "Practice a modest amount of due diligence," recommended Tzanis. "Just run the address; just run the phone number. If

you Google either and they're supposed to be from a well-known company but there's no match, then it's probably a scam."

"The first point is that if it sounds too good to be true, it probably is," added Coe. "I don't know if we'll ever be able to prevent it from happening. I think it's going to be more of an educational type of thing on the part of the potential victims. They are the ones that are going to have to look out for themselves, because it's going to happen and it continues to happen."

**Reprinted from NACM's Business Credit magazine, June 2008. Originally written by Matthew Carr, former NACM staff writer.*