

Are You Fighting Fraud?





You can do something about it.

First, admit that you might be a victim.

By Susan L. Hodges

In less than one week, a single defrauder can make a fortune.

And unless you're on top of your game, your company could become a five-star contributor. Thanks to advancing technology and competitive pressure that rewards speedy transactions, fraud can be easy, fast, and highly rewarding. By the time a lessor discovers his new customer is fake, the "fraudster" can be sipping martinis in Monaco. At least it's reasonable to assume so, since for every 700 cases of consumer identity theft, only one is solved. This is not to say that the leasing industry is any more at risk than other financial service providers. Every day, U.S. lessors conduct about \$1 billion worth of business, and only a tiny fraction is suspect. Still, there are some high-profile cases in the news. And it's not just legitimate businesses that benefit from new technologies and the increasing pace of business.

Sophistication

Ajay Pillai, associate principal at Inductis, a Providence, New Jersey-based consulting firm, says commercial fraud can be even easier to commit than consumer fraud. To create a business identity, Pillai says anyone can go to the office of any secretary of state, or visit its website to find a business that's no longer active." You



When fraud professionals discover a company with few deterrents in place, transaction size is not an obstacle.

may then be able to buy such a company for pennies on the dollar, or just steal its identity,” says Pillai.

To create a business identity, you can register the name with the secretary of state by completing a few forms, and possibly obtain a D&B number online using an address and phone number. Says Pillai, “You can create a trail of activity that gives the appearance of a legitimate business. Then you can go after a number of providers and defraud them all in a relatively short period of time.”

“Are [defrauders] becoming more sophisticated? Absolutely,” says Dennis

Jeffries, vice president and chief credit officer for Great America Leasing Corp., a small-ticket leasing company in Cedar Rapids, Iowa. Due to the nature of the business, small-ticket companies are still favorites of defrauders. The scant documentation requirements of some companies for individual transactions, the increase in automated credit-scoring, and the impracticality of inspecting each piece of equipment can place small ticket firms at big risk. Also attractive to defrauders are assets that are easily moved or liquidated, such as computers and other small electronics.

But when fraud professionals

discover a company with few deterrents in place, transaction size is not an obstacle. Whether the ticket focus is large, medium or small, that company becomes a target. One consulting firm that has tracked fraud in leasing companies says that of an estimated 30,000 to 40,000 leases written daily, roughly 100 to 200 are fraudulent.

“The more automation used in the decisioning process, the less likely applicants will be picked up for fraud,” says Dan Rucker, managing director of fraud detection and prevention solutions for D&B (formerly Dun & Bradstreet). Intelligent fraudsters can slide right through most credit screens—and when they do, their success is nearly guaranteed. So lucrative is professional fraud that Rucker says it is becoming a profit center for organized crime and perhaps even for terrorists. The smartest defrauders constantly monitor anti-fraud procedures used by leasing and finance companies and gravitate toward the ones with the least resistance. Says Rucker, “If lessors aren’t using the best available tools to fight fraud, they could find themselves in bad shape.”

Vicious Vendors

A particularly insidious form of fraud is that committed by vendors. In a typical lease transaction, a vendor receives the lessee’s information and



then may submit the deal electronically to several lessors. All vying for the business, lessors compare the information to their credit requirements and shoot back a quick response. In the rush to get new business, good judgment can take a back seat.

In vendor fraud, victims may include the lessee as well as the lessor. But occasionally, both vendor and lessee benefit. Such is the case when a vendor agrees to inflate a purchase price and receive a kick-back from the lessee. Susan Rosenthal, a partner at Brown, Raysman, Millstein, Felder & Steiner, LLP, in New York City, says this happens a lot. "If the lessee can't pay the vendor, but needs to lease equipment, the two parties get together and say that the equipment costs more than it does," she explains. Or the lessee may have already leased equipment and now wants an unsecured loan, but doesn't believe he can get it through legitimate means. In this case, he and the vendor may agree to fabricate the equipment so the lessee can get the money he needs.

More common, says Rosenthal, is the falsification of financial statements. Here again, defrauders are gambling that the due diligence of the leasing or finance company won't be rigorous enough to verify the information on an application. They often win. "In many instances, no one can afford to do that much due diligence," says Rosenthal.

Train Your Staff

Difficult as it is to detect and prevent fraud, there are steps leasing and finance companies can take to make their firms less vulnerable. Staff training is one, because although approaches to fraud have become slicker, the types of fraud committed and the red flags

they raise are still much the same:

- a company orders more laptops than it has employees
- a previously inactive client suddenly applies for new business
- a vendor charges an inflated price for equipment
- a vendor or lessee attempts multiple financing for one piece of equipment.





Defrauders are gambling that the due diligence of the leasing or finance company won't be rigorous enough to verify the information on an application. They often win.

When Dennis Jeffries or his employees detect such activity—and they are trained to do so—they use two search engines (Anywho.com or Switchboard.com) to cross-reference the applicant's phone number and address. For a fee, these search engines provide a wealth of data, from bankruptcies and tax liens to 10 years of phone numbers and addresses. Says Jeffries, "Just taking the time to determine whether a phone number represents a business address or a residential one has

helped us immensely." The company has detected and rejected several suspicious applications in the last 18 months.

"Training your credit department is crucial," confirms Curt Zoerhof, chairman of ELA's Credit Committee and senior vice president of Wells Fargo Equipment Finance, in Minneapolis. "Credit professionals may have all the degrees in the world and be able to crunch numbers better than anyone, but those things are no substitute for experience."

Analyze Your Data

The challenge, of course, is to balance good service and timely turn-around with smart strategies that detect and deter attempts at fraud. Screening every applicant for fraud is not only cost-prohibitive, it also deters legitimate customers who want equipment or capital without a hassle. What you can do, however, is peruse your data to identify the 5 to 10 percent of transactions that need extra attention. Scrutiny often reveals patterns in suspicious transactions. You can then build one or two new questions into your applications that may deter defrauders but won't pose difficulty for legitimate customers.

While lessors can detect and deter many amateur attempts at fraud, uncovering the schemes of professional defrauders is harder. "If we have an entity that has paid fees to acquire an old corporation, set up a new address near the old one, and [registered] with D&B, it's hard to see the fraud," says Jeffries. "Occasionally we're going to get burned."

Investigate Selectively

To fight professional fraud, investigate the cause of selected defaults and then implement new policies that specify when and how to conduct background checks. Also consider appointing one or more credit special-



While lessors can detect and deter many amateur attempts at fraud, uncovering the schemes of professional defrauders is harder.

ists as investigators. “It’s foolish not to find out if you’re being defrauded,” says Dennis Jeffries. “If you don’t do anything [to change your procedures], you’re going to get hit again.”

Again, lessors may groan at the cost of investigating any one transaction. “But almost every lessor can give an example when they first learned of a fraud and took immediate action, and were able to recover,” says Curt Zoerhof. You owe it to your company to enforce your liens and close your assets.

Another investigation worth doing is a review of transactions generated

by each vendor. By conducting such a review every quarter, or as often as every month, equipment leasing and finance companies familiarize themselves with the habits and eccentricities of each vendor, thereby making it easier to identify information or procedures that seem out of place.

A third form of investigation is kicking the tires. “Hardly anyone goes out to meet people or inspect the equipment, but you need to do it sometimes,” says Susan Rosenthal. One approach is to conduct one inspection per vendor each month or each quarter. At the

very least, she advises, pick up the phone and talk to the vendor. “Have your antennas up,” she says. “Ask questions about the equipment [and the lessee] to help ensure they exist.”

Rosenthal also suggests using extreme care in the execution of documents. “The days of issuing docs in advance are over,” she says. The longer the time between document execution, payment and equipment delivery, the greater the opportunity for fraud. No matter how well you know the vendor or the lessee, it’s almost never wise to do a “favor” by sending completed paperwork up front.

Who’s Responsibility?

Whether or not your credit department should carry the entire burden of fraud prevention and detection is a matter for debate. Although many lessors—and credit departments—are comfortable with the responsibility, that doesn’t mean it’s always a good idea. As Dan Rucker points out, “In credit, you assume the data you’re looking at is true. In fraud, you try to determine how true the data is, and what needs to be validated. Fraud detection requires a special set of skills and tools.”

Of the D&B customers Rucker has interviewed, about half use their credit departments to identify and protect against fraud while the other half uses a separate anti-fraud group or security



group that works outside the credit department. At Wells Fargo Equipment Finance, Zoerhof uses his parent company's centralized credit investigation system. At Great America Leasing, CEO Paul Usztoek relies on both his credit department and his operations staff to watch for fraud and report red flags.

Ajay Pillai believes that the higher a company's business volume and the larger its transactions, the stronger the case for having fraud specialists. "You need different methods for verifying information and checking backgrounds," he says. "It's a different job."

Automated Solutions

To help lessors and finance professionals in their detection efforts, D&B will soon introduce new anti-fraud solutions that rate the likelihood of an applicant to commit fraud. "We're going to look more at the behavior of the fraudster than at the application data," explains Rucker. The D&B tools will use technology and analytics to perform leading-edge fraud-detection techniques. D&B's offering is designed to help lease and finance companies with small to medium business volume.

Firms with higher volume may be interested in a customized solution designed and built by the consulting firm, Inductis. Ajay Pillai says Inductis helps clients analyze their data to determine which types of applicants are most

The longer the time between document execution, payment and equipment delivery, the greater the opportunity for fraud.

likely to commit fraud. The company then creates an automated, statistically based screening tool to evaluate every new applicant and identify those with high-risk ratings. Information on these applicants is then fed through manual fraud checks in credit origination, booking and funding. By rapidly screening new applicants and identifying those at risk, the lessor can avoid the expense and labor required to implement greater due diligence across the board.

Each solution is set to detect irregularities at a level the client can support. In other words, Inductis programs the model's working parameters at the level most cost-effective for the client.

Recourse

Because equipment lessors and finance professionals believe there is little they can do about fraud once it has occurred, they often do nothing. Marc Hamroff, managing partner at Moritt, Hock, Hamroff & Horowitz, LLP, doesn't believe that's always wise. "You have to think about alternative credit recoveries," says Hamroff. "If the vendor participated in the fraud, for example, you may have recourse [against the vendor]."

Accountants can be a source of recourse as well. Recent legislation imposes greater burdens on accountants to create financial statements that are accurate and don't mislead.



At the same time, both Hamroff and Susan Rosenthal admit that suing fraudsters can be expensive and time consuming. "Fraud is very hard to prove, because it requires intent," says Rosenthal. Fraudsters transfer their assets and there may be nothing to sue against. "Unless you know there's a pot of gold at the end," Rosenthal adds, "you may not want to go through with it."

Marc Hamroff believes lessors focus too much on credit scores. Instead, he thinks more emphasis should be placed on checking the authenticity of new customers. "We know it's hard," he says. "The challenge is to find a balance between being quick, profitable and productive, and being more careful." By using certain of the tools discussed here, equipment leasing and finance companies of every size and market segment may be able to do just that. **ELT**

Susan Hodges of Silver Spring, Maryland, writes about leasing and other topics. Contact her directly at hodgeswrites@aol.com.