

Business Credit[®]

National Association of Credit Management

THE PUBLICATION FOR
CREDIT AND FINANCE PROFESSIONALS

April 2003
\$7.00

BUSINESS CREDIT

Selected Topic

Hidden Opportunities in Credit Fraud Risk Management

By Gary Bares

In recent years, open-terms credit fraud has become a tremendous threat to a widening circle of businesses and industries. In fact, it is not uncommon for companies in some industries to experience fraud loss rates equal to 25 percent or more of overall bad debt. Trends in technology, law enforcement and the Financial Value Chain (FVC) have facilitated this growth and are unlikely to slow. At a time when competitive pressures are forcing companies to cut costs and identify additional opportunities for differentiation, credit fraud prevention has come to the forefront.

Credit Fraud Dynamics

Open-terms credit fraud attempts total nearly one billion dollars annually in the United States and continue to increase in sophistication. It is not uncommon for perpetrators of this fraud to be linked to organized crime groups who favor it over traditional criminal activities that receive greater law enforcement priority. Its popularity has also been increasing among less sophisticated criminals, and trends fueling this growth are likely to continue.

Credit fraud perpetrators operate by studying and manipulating the resources traditionally used in the credit decision process. The fact that many businesses use credit reports based largely on self-submitted or related party data makes it a perfect environment for fraud. Since many of the credit resources and accompanying processes have changed slowly over the

years, perpetrators have had ample time to perfect their craft. Fraud has few allies as important as consistency.

Credit fraud schemes vary considerably, but generally fall into three categories. These include (1) organizational identity theft, (2) shell company fraud, and (3) bust-out fraud. Organizational identity theft is generally the least sophisticated of these schemes, while bust-out fraud tends to be the most sophisticated.

Organizational identity theft is a fairly basic scheme with the perpetrator assuming the identity of a legitimate and creditworthy organization. Advances in desktop publishing have greatly aided this type of fraud, as documents from the perpetrators can be nearly identical to legitimate ones. The speed of commerce and the growth of Internet-based relationships further enable these schemes.

A more sophisticated type of credit fraud involves using one or more "shell" companies existing mainly in appearance or structure. A recent fraud of this type also included a fictitious bank complete with a directory assistance listing. Perpetrators hope that credit grantors will be fooled by company websites, phone listings, incorporation data, seemingly independent trade references and credit reports based on self-submitted data. Once the scheme is complete, the perpetrators simply close up shop and disappear. These parties frequently choose locations based upon this exit strategy, often

operating in large cities where credit fraud receives less attention from law enforcement.

The most sophisticated and capital-intensive scheme type is bust-out fraud. This fraud involves either building or acquiring a company for the purpose of using its good credit rating in a fraudulent manner. Once perpetrators control such a company, they embark upon a purchasing spree with no intention of paying the final bill. The product is then disposed of through channels established prior to the actual bust-out. Some of these schemes can take a year or more to unfold.

Contributing Factors

A number of contributing factors have aided the growth of credit fraud in recent years. Trends in FVC dynamics, Internet commerce, customer base, law enforcement priorities, and credit employee mobility have combined in favor of the perpetrators. These trends are unlikely to slow.

At the organizational level, trends in the FVC, including increased speed and automation, are adding greater complexity to fraud prevention. These elements combine in favor of the perpetrators who thrive in such an environment and adjust their strategies accordingly. The automation of certain FVC functions not only has implications for general fraud risk but can also increase system predictability. Such systemic consistency increases the risk that perpetrators may repeatedly exploit vulnerabilities.

The emergence of Internet commerce, particularly the auction sites, has driven the spread of credit fraud to new industries. The popularity of these sites increases product liquidity and makes it easier for perpetrators to dispose of goods. The anonymity provided by the Internet also adds to its appeal, as does the ability it provides to easily set up credible looking company web sites.

Solution Dynamics

Accurately quantifying the extent of the problem is the first step in moving towards effective prevention. One complicating factor, however, is that unlike credit card fraud, open-terms fraud losses are often not recognized as fraud. This is especially true for schemes ending in bankruptcy. Collaborative organizations such as the NACM Loss Prevention Group can be extremely helpful in determining if a particular loss is fraudulent in nature. Such collaboration can also help to determine the extent of victimization across an industry, which can be critical when approaching law enforcement.

Once awareness and accurate quantification have been established, companies typically ask three basic questions: (1) How real is the continuing threat to our company? (2) What are the elements of effective prevention? (3) What level of prevention success can be achieved?

The actual threat of credit fraud is typically much greater than companies realize. A recent example from a billion-dollar computer company perfectly illustrates this fact. An internal investigation at the company revealed that from a national list of 350 frauds spanning an 18-month period, the company had received credit applications from 48, had granted open-terms to 19, and had lost nearly one million dollars to the frauds. Ironically, prior to the investigation, the company denied having a significant credit fraud problem, instead attributing mounting bad-debt losses to an increase in customer bankruptcies.

The optimal combination of solution elements for a company will depend on a number of

variables including, but not limited to, exposure dynamics, loss history, organization size, market served, order receipt channels, product mix, product margins and FVC dynamics. Failure to consider all of the factors involved is one of the leading causes of low return-on-investment (ROI) for fraud prevention efforts. Frequently, the most difficult part of this equation lies not in detecting fraud but in finding the optimal balance between competing organizational objectives.

Experience shows that great success can be achieved in credit fraud prevention by combining aggressiveness and innovation. One multi-billion dollar technology company recently experienced a 30 percent decrease in bad-debt losses (savings of one million dollars) after establishing a centralized fraud prevention presence. The ROI for this endeavor was nearly 1500 percent in the first year alone. Aggressiveness and innovation are the keys to achieving such levels of success.

Prevention Elements

One fact that works in favor of prevention is that perpetrators have historically faced little resistance in the form of aggressive prevention. Because of this, the perpetrators themselves have become somewhat predictable and experience shows that few are prepared for innovative prevention efforts. In fact, these fraud schemes tend to be very sloppy beneath the surface level and this has been one of the most surprising discoveries of prevention professionals.

Though fraudulent attempts may appear legitimate and creditworthy on the surface, using Internet-based tools to dig a little deeper can reveal major surprises. Such tools can also help to interpret intent, which is often the only criminal element in the early stages of a scheme. Clever use of these technologies also allows a business to determine whether an applicant has the infrastructure in place to be operating as they claim to be, and whether they have a presence in the communities and markets they claim to serve. These processes can usually be carried

out in a matter of minutes and nearly all of the tools are either free or relatively inexpensive.

A national negative database such as that provided by the NACM Loss Prevention Group is one example of the tools available for prevention. Searching a historical database such as this can reveal prior fraudulent activity by a business, principal, or scheme type. A recent study by Verifraud, Inc. demonstrates just how valuable such a database can be. This study, based on a sampling of two hundred credit fraud attempts, found that 22 percent could be directly linked to previous credit fraud activity. In fact, one fraud from the study which victimized a computer company for one million dollars was stopped by another after a search revealed a similar scam in the area two years earlier, using the same method of operation along with some of the same out of state references. Surprisingly, many perpetrators do a poor job of covering their tracks.

Though individual tools such as a historical database are critical, they are hardly sufficient in and of themselves. With credit fraud increasing in complexity, experience shows that successful prevention is achieved by using a wide array of tools in conjunction with innovative strategies and processes. Furthermore, these elements must be positioned seamlessly within existing business processes while remaining consistent with broader organizational objectives.

Summary

Though credit fraud poses a growing threat to businesses across many industries, the news is not all bad. Effective prevention methods are available and their successful implementation can actually be a source of competitive advantage. By combining aggressiveness and innovation with a sustained resource commitment, organizations can turn credit fraud prevention into an area of tremendous opportunity.

Gary Bares is president of Verifraud, Inc. He can be reached by e-mail at gbares@verifraud.com or visit www.verifraud.com.