What seems like bad debt could simply be fraud. Knowing which is which can help collection efforts.

By Carolyn Hardin-Levine
Director, Commercial Fraud Solutions, EXPERIAN

IDENTITY THEFT AND OTHER forms of fraud have understandably commanded significant media and regulatory attention, but a large amount of fraud flies under the radar, going undetected as bad debt.

Industry executives Experian has talked with estimate that some 30 percent of all commercial credit losses can be attributed to false or misleading information that went undetected through the approval process. Some put such “soft” fraud losses as high as 40 percent to 50 percent.

That means a large chunk of bad debt could be mitigated if there were a way to differentiate fake from factual information. This raises questions for the commercial credit industry.

What effective methods are there for properly identifying fraud versus bad debt?

How can sound fraud risk strategies reduce needless losses and improve back-end collection efforts?

That’s important because the more accurate the information obtained and acquired on the front end, the easier the collection efforts are on the back end.

To understand the true depth of today’s commercial fraud problem, one cannot simply analyze the small quantity of transactions that have been definitively identified as fraud. It’s important to analyze the types of fraud triggers that are hidden in bad debt.

In other words, find a way to segment out the “soft” fraud so it can be treated accordingly. Experian late last year undertook a study to do just that.

In the study, done in September 2005, almost 17,000 bad debt commercial accounts were analyzed. Bad debt was defined as more than 90 days delinquent or worse reported within the last 30 days. These accounts were contributed by 770 different companies and represented almost $620 million in total commercial losses.

Not surprisingly, the average bad debt balance was more than five times greater than the average good account balance reported by the same companies. The businesses’ names, addresses and phone
numbers were used to search for patterns that would indicate fraudulent or misleading information. Then those patterns were compared with similar analyses conducted on the good-performing accounts. The businesses’ names, addresses and phone numbers were run through multiple processes:

- Telephone and area code data to match the business name and address.
- U.S. Postal Service address standardization and delivery sequencing, showing when an address is a non-existent building or suite number or a vacant lot or if the city, state and ZIP Code do not match.
- Business name, address and telephone data where the information was verified by at least two independent sources to ensure that a business exists.
- Business addresses and phone numbers deemed high-risk based on industry surveys to identify the use of a potential false front address, such as storefront mail-receiving facilities, drug rehabilitation facilities, bars, etc.

The results were clear. A great deal of fraud does indeed go unidentified and ultimately ends up misclassified and worked as bad debt. When treated as traditional bad debt, fraud accounts dampen an otherwise effective collection effort and can needlessly waste traditional recovery resources.

High-risk address and phone numbers were found to be key indicators of potential fraud. When the address was identified as high risk, the average bad debt balance was six times higher than on similar good accounts.

When the phone number was named as a high-risk address, the findings were even more significant. The average loss with this indicator was more than double the average loss and almost 23 times greater than the average good account balances with the same indicator.

The phone number proved to be valuable in other ways. When the business name fails to match the phone number listed for the business, the average bad debt balance is four times greater than the average for all other bad debt. Further, those triggers corresponded with a very small balance on the good accounts in this category.

Entities trying to deceive often provide information that on the surface looks plausible. Looking More Closely

Yet when that information is closely scrutinized with other application data, other potential fraudulent indicators start to emerge. The best authentication tools look for these anomalies to pinpoint inaccuracies.

Such anomalies also were identified in this study. Some of the indicators of fraud that surfaced are obvious, such as a business address that turned out to be a vacant lot. Other anomalies were far subtler. Address numbers were found that did not exist on the street given, or street name, city, state and ZIP Code types of mismatches emerged.

Comparing the business data elements against each other produced even more suspicious triggers, such as the phone prefix not matching the same geographic area as the ZIP Code on the address. Some of these anomalies again produced dramatic results, with one such indicator revealing an average bad debt balance 88 times greater than the average good account balance in that same category.

By combining these indicators, one can further refine the process by discerning clusters of fraud triggers that indicate a more precise blend of characteristics to identify false and misleading information. The study revealed that these clusters of fraud triggers produce even stronger results.

More than 28 percent of all the bad debt reviewed fell within less than 15 such fraud trigger clusters, while less than 10 percent of the total population had those same indicators. Considering that the accounts evaluated were not known frauds but bad debt accounts, these findings were dramatic.

A truly robust commercial fraud risk strategy uses similar analysis and processes on all of the applicant’s data. It is not uncommon, for example, for business transactions to include multiple addresses. These addresses on the application may appear as additional business locations, billing addresses or ship-to locations.
Many mid-size to small businesses also have personal guarantors who bring in consumer identification information to validate. Business transactions typically have business tax identification numbers and the guarantor’s personal Social Security number as well.

A fraud risk strategy that scrutinizes all such elements together makes fraud indicators more clear.

**A Case Study**

To take this premise to the next level, a similar study was conducted last September jointly with a financial institution on the impact of fraud screening when used on all the application information. In this study, two small-business loan portfolios’ performances from the same financial institution were compared. One portfolio utilized a robust fraud screening process. The other used none. Again, the potential fraud indicators were grouped into unique clusters.

Not surprisingly, the good accounts performed similarly across all clusters in both portfolios (see page 39). However, the portfolio that used fraud screening had a significantly lower occurrence of bad debt across all clusters evaluated.

More importantly, the portfolio using fraud screening was approving higher credit limits, had higher utilization ratios and could provide more accurate information for the collectors when an account did go bad.

A truly good fraud and authentication process will not only look for the indicators for false and misleading information, but also provide the actual data that produced those indicators. This data can be invaluable and provide much needed insight for collectors.

For example, let’s say the business lists a phone number on the application. The fraud screening process produces an indicator that the phone number cannot be independently validated or matched to that business.

Perhaps the originating credit analyst doesn’t think that this is unusual as he or she used that phone number to reach the applicant and decides to approve the transaction. The fraud screening results subsequently are filed as part of the overall credit review documentation. But then, that customer doesn’t pay.

It would be valuable information for the collector to know that the reason for the warning indicator on the phone was because it was listed as a mixed-use phone. It also would be useful to provide the name and address of the company the phone number was listed for.

When one has the tools and data to distinguish between good information and bad information, recovery staff can more effectively focus efforts only on those accounts that have the highest potential for collection. Similarly, fraudulent accounts can be quickly identified and managed accordingly. Amazingly, however, many companies do surprisingly little to identify fraud.

In a recent survey of 120 commercial credit executives, more than 70 percent reported that fraud is a concern to their company. The overwhelming problems they encounter are false or misleading application information, first-time payment default (for reasons that cannot be identified), fictitious identity of a business and identity theft of a business or the personal guarantor.

But when asked what their companies do to identify fraud, no clear difference emerged between how they approach credit risk and fraud risk. Most companies still rely on a manual review of the same information sources used for credit underwriting, perhaps looking at a single source such as a credit report.

About 40 percent check public sources such as secretary of state records, but those are easily compromised because incorporation papers can be easily falsified. Remarkably, some 15 percent report having no fraud identification processes whatsoever.

A thorough fraud risk strategy clearly augments and complements credit risk policies and approval processes. While reducing bad debt, it also creates clearer separation between true fraud losses and regular credit losses, providing more accurate and comprehensive information on businesses for recovery staff to work with.

In short, a more robust fraud risk program helps collection efforts become more effective and focused.