

Fraud and abuse involving corporate credit cards are more frequent and more subtle than most managers realise. Typical schemes for misusing corporate cards depend on weak internal controls, such as accounting systems that collect the telltale clues, but never connect them. Here are some fairly simple techniques that will help.

The key is to recognize that every credit card statement line item must first be verified and then tied to some legitimate corporate activity. The itemized monthly reports issued by your card provider will rarely be sufficient to accomplish either, but they are the logical place to begin.

For example, data can be sorted by card number, after which the date field can be checked for:

- (a) multiple purchases on the same day (using the Duplicates command);
- (b) purchases on weekends or statutory holidays (using the CDOW() function); or
- (c) a trend toward more frequent purchases (using the AGE() function).

All this takes just moments with a proper batch file in place. This type of testing will also help to identify stolen cards or card numbers being used in widely separated locations, as well as attempts to circumvent spending limits by breaking a large purchase into pieces. However, even if the results of the testing seem to point towards fraudulent activity, the activity could be legitimate, depending on company policies and practices.

For example, trucks that are on the road all day may need to fill-up on fuel three times in 24 hours, and traveling salespeople frequently conduct business on Saturdays. In these cases, the filters and conditions can be adjusted to reflect company practices.