

## Computer Fraud--How To Find It

Computer technology has made fraud a growth industry of the 1990s.

Incidents of fraud being perpetrated through the use of computers are increasing. In many organizations, anyone with rudimentary knowledge of a company's computer system is potentially capable of illicitly accessing sensitive information--or worse. Estimates are that, in 1999, fraud will cost U.S. businesses over half a trillion dollars, with much of that being the result of computer crime.

And, computer fraud does not only affect a company's bottom line. Many company executives and outside directors are learning the hard way that they may be held liable for the lack of internal programs to prevent or minimize the impact of computer fraud.

### Searching for Computer Fraud

Fortunately, most computer fraud is perpetrated by relatively unsophisticated individuals. Evidence of the fraud is difficult to hide, especially where a specialist in computer forensics is involved in the search. These specialists are trained to identify and preserve electronic data that can later serve as evidence in court.

The telltale evidence of fraud is commonly left behind on hard drives and floppy disks. As with most computer users, those who commit fraud assume they can erase incriminating files by simply deleting them from the storage medium. But truly deleting a file is not so easy. Often, a file on a network or individual computer is automatically backed up by a tape drive or other means as a part of a disaster recovery plan. Moreover, with computers using recent Microsoft Windows(r) operating system software, for instance, deleted files are generally placed in a "recycle" folder where they can be easily recovered.

Even where files have been allegedly deleted from the computer, it is still possible to recover data. Most operating systems delete files by simply removing the first letter of the file name and deleting reference to the file in the file management system. While the operating system does not recognize the file, it is still physically present on the storage medium. Sophisticated software can retrieve this data.

Even files that have never been saved on a computer's hard drive may be recovered. This "ambient data" can often be found in so-called "temp" files stored on the computer's hard drive. For example, a fraud perpetrator may view documents (say, files stored on a company's e-mail server) on a computer without saving those files. However, all or portions of the viewed documents may be stored in temp files on the perpetrator's computer hard drive.

## Broad Knowledge Is Essential

Computer technology has made fraud a growth industry of the 1990s. It takes more than computer know-how to effectively search for, preserve, and present evidence of computer fraud. Forensic accountants with computer expertise can help determine how the fraud was committed, assess the damages, and provide the expert testimony needed--as well as assist the company in devising ways to prevent similar fraudulent activity in the future.