How to Use Computer-Assisted Audit Techniques to Uncover Fraud

By:
Tommie Singleton, Ph.D., CPA, CISA, CITP, CMA
Kelly Todd, CPA, CVA
Frank Messina, DBA, CPA

According to the Association for Certified Fraud Examiners (ACFE), fraud is estimated to average 6 percent of total revenues in the United States. That statistic is from the association's "2004 Report to the Nation," which surveyed hundreds of Certified Fraud Examiners (CFE) to empirically examine the level of fraud in the United States. Much of this ongoing fraud is associated with check writing or fraud schemes that could occur in banks. The same report also identifies the common methods of detecting fraud. The tips and complaints system is still the most common method of fraud detection, but internal audit now ranks as the second most common method to successfully ferret out fraudulent activity. Moreover, a common tool for fraud detection used by internal auditors is computer-assisted audit tools and techniques (CAATTs), such as generalized audit software (GAS). This article examines several of these audit tools and techniques that can be used for fraud detection.

The most common form of CAATT used in the information technology (IT) audit profession is GAS. This software allows the auditor to examine 100 percent of the data in transactions, not just a sample, and to conduct a number of audit techniques that have evolved over the years and have been proven to be effective in detecting anomalies that could be indicators of fraudulent activity.

These commands in GAS associated with audit techniques have evolved over the years, many times by trial and error. The techniques discussed herein have been proven to be associated with various common fraud schemes of the past and present.

Data Filters. One GAS technique is commonly referred to as a *filter*. A filter is set to choose only those transactions that match or meet a certain criteria. For example, if a bank has a pre-set limit of $50,000 for loan officers before the loan goes to the loan committee for approval, the filter would choose those loans that were just below $50,000. Prior frauds have been perpetrated by loan officers making bogus loans just below the authorization level to maximize the amount of the theft. Filters can also be used to spot data that is not there but should be, such as missing data values. Another potential GAS example would be to search for checks where the payee, check signer, and endorser/depositor are the same person. Of course, this assumes that this data is available. Fraudsters sometimes write checks to themselves and then deposit the checks into their own bank accounts. Thus, it is possible to identify fraudulent checks of the bank's customers if this procedure is feasible.

Data Sorting. Another GAS technique is *sorting*. This technique is employed by sorting all transaction data, thereby allowing the reader to instantly spot certain data anomalies in the sorted transactional field. For example, sorting all transactions by date can help spot dates that are too old or yet in the future. Sorting can also help identify transactions outside the normal range of values.

Statistics. A third technique used to detect fraud is the regular use of *statistics*. Generating descriptive statistics for all transactions can be effective, but the reader or auditor must understand the meaning of terms such as mean, standard deviation, and the 95 percent confidence level. For example, it is easy to identify *outliers* if the reader can mentally calculate the distance from the mean, or average, that the 95 percent confidence level will extend numerically by multiplying the standard deviation times by approximately three, and adding and subtracting that amount from the mean. Any transactions with amounts above or below the 95 percent range are technically outliers and are possible anomalies. Even if not an anomaly, that transaction should be examined because it is outside the *normal* range of transactions. Statistics or filters can identify negative or zero values where none should exist. For instance, using the statistics function of the GAS or a filter to see if any deposits are zero or negative would clearly be an anomaly.

Duplicates and Gaps. A fourth technique is *duplicates and gaps*. GAS commands include duplicates for locating duplicate transactions, which would be an anomaly. Thus the auditor can locate any duplicate deposit transactions that have been posted in the database. The same could be true for locating gaps or missing transactions such as checks or deposits. Duplicates and gaps find transactions that are not sequential where they should be sequential, or find sequential transactions where none should exist.

Aging Analysis. The *aging* GAS technique is useful for locating transactions where the age of the transac-

tion can determine if it is an anomaly. For example, if a deposit in transit has a date that is three-months-old, it clearly would be an anomaly. Aging analysis can be used by bank tellers to ensure that fraudulent theft of cash is not being covered-up by paper documents in the drawer.

Character Classification. Another GAS technique is *classify*. Classify gathers transactions by a character field, such as teller or keypunch operator ID. When percentages are calculated, the auditor can assure that certain transactions are normally distributed across the employee population. For example, if 80 percent of all credits to accounts are by the same person, and the bank has a dozen or so operators, this revelation might just be an abnormal percentage. Character classification can also help in spotting anomalies using depositor or payee as the source of the statistic.

Stratifying Data. *Stratify* is a GAS technique that distributes transactions across equal layers of amounts. By examining these layers, or strata, the auditor can spot certain anomalies. If the distribution is abnormal, it can be seen and the auditor can follow up to see if the abnormal distribution is indicative of one or more anomalies.

Benford's Law. The eighth and final GAS technique is Benford's Law. It seems plausible that the probability of any number being the first digit in an amount is the same as any other number, but research has proven that to be false. The digit 1 is much more likely to be the first digit in an amount than the digit 9. Benford's Law is the result of this research and identifies the probability of any digit being the leading digit. GAS contains a command to execute Benford's Law across a database with a chosen amount field and report the percentage of occurrence for each digit, then compares the distribution to the normal probabilities. If fraud exists in the data, it is possible it will affect the percentages of distribution of leading digits. For example, one fraudster used the digits 99 to identify fraudulent transactions for purposes of the perpetrator, that is, so the perpetrator could track the phony transactions. Benford's Law would have shown a clear anomaly in the percentage of occurrence of 9 as the leading digit, or 99 as the leading two digits, versus what that percentage should be in a normal file.

Conclusion. The use of these GAS techniques is not a cure-all, nor does it necessarily identify fraud. Rather, it directs the attention of the trained IT or fraud auditor to identify possible anomalies. Anomalies in data are the result of only two types of problems, including a) errors or b) fraud.

Some of the popular vendors of generalized audit software include ACL (*http://www.acl.com*), Pan Audit (*http://www.ca.com/*), and Idea (*http://www.caseware-idea.com/*). Using one of these CAATT tools can be very effective in detecting fraud, especially since these tools examine 100 percent of the transactional data.

Understanding Internet-Based Fraud Schemes

By Reese Issle
Wachovia Corporation

Since late 2002 there has been a significant worldwide increase in the use of computer and Internet technologies that are employed by cyber thieves to compromise individuals' identity and financial information. Organized criminals and fraudsters are frequently using information technology to perpetrate financial crime. In the past 18 months it seems that almost everyone with an Internet-based e-mail account has been solicited by one of the following schemes:

- received a phishing e-mail;
- had a computer virus placed on their computer;
- saw, navigated to, or heard about a fraudulent Web site that put malicious code on the individual's computers; or,
- had debit, credit card, or checking account information compromised because a small- to medium-sized merchant processor had either been hacked into or had their digital transmissions intercepted.

Technology has become a double-edged sword. One edge gives us access to a world of information and products that are just a click away. This world promises efficient, smooth access to readily available worldwide data. The other edge of the sword uses this same access to data and technology to compromise proprietary financial data and commits financial crimes.

Phishing Schemes Abound. The growth in phishing attempts, virus production and attacks, and the sheer number of hacking cases suggest that the financial services industry is approaching the critical tipping point where technology mediated crime is becoming a favored technique of criminals. These technology-mediated crimes present thorny problems in terms of