



How much is your organization losing to undetected fraud?

“AuditExchange’s managed analytics platform will allow our Fraud, Surveillance, and Audit teams to work together seamlessly and bolster our fraud prevention programs to avoid unnecessary data duplication and improve reporting procedures.”

George Fischetti

Data Analyst/Senior Fraud Investigator
MetLife Special Investigations Unit

Fraud Detection

A typical organization loses 7% of its annual revenues fraud. In the United States, this translates to fraud leakage of approximately \$994 billion yearly.

This is according to the Association of Certified Fraud Examiners’ *2008 Report to the Nation on Occupational Fraud and Abuse*, which covered 959 occupational fraud cases. Sixty percent of the frauds in this study involved losses of at least \$100,000 and more than 25 percent resulted in losses in excess of \$1 million. In addition to the direct dollar costs of fraud, organizations must cope with a range of indirect costs. Damage to a company’s reputation can have substantial fallout – and lead to punishing market setbacks. Loss of customer confidence translates directly into reduced revenues and profits. And employee morale can suffer, impacting organizational productivity and the ability to attract and retain qualified staff.

The nature of fraud

The ACFE defines fraud as “the use of one’s occupation for personal enrichment through the deliberate misuse or application of the employing organization’s resources or assets.” In simple terms, frauds fall into three broad categories: asset misappropriation, corruption, or fraudulent statements.

The vast majority of frauds surveyed in the ACFE study, nearly 90 percent, involved asset misappropriation such as revenue skimming, inventory theft and payroll fraud, averaging a median loss of \$150,000.

How fraudsters exploit complex systems

The KPMG *Fraud Survey 2006* reported that of the factors contributing to fraud in the organization, “poor internal controls” rated as the highest at 33 percent, and “override of internal controls” rated second at 24 percent.

Typically, fraudsters detect or stumble upon areas with weak cross-departmental or cross-organizational controls, often the site of the interfaces between two or more computer applications or systems. The perpetrator is confident that there is very little regular cross-system validation, given the challenges inherent in accessing and analyzing frequently incompatible data formats.

Many organizations lack the in-house capability to carry out such complex tasks efficiently and in a frequent, timely fashion. The complexity of finding fraud grows when there are multiple systems involved.

In many organizations, both systems and their underlying transactions have become increasingly complex, with data volumes growing at an exponential rate. While strong internal controls and audit procedures play a role in preventing and detecting fraud, it is unrealistic to assume that they are completely effective. For many organizations, there remains a strong likelihood that a significant number of frauds are simply never detected.

Even when frauds do come to light, many detection methods, such as audit procedures, only occur some time after the fraud has taken place. The longer frauds go undetected, the larger the financial loss is likely to be and the smaller the chance of recovering the funds or assets from the perpetrator.

Building a better mousetrap: use technology to analyze every transaction

Associations and leading audit organizations all advocate the use of data analysis technologies to assist in fraud detection. Data analysis technology allows auditors and fraud investigators to obtain a quick overview of the company, develop an understanding of relationships between various data elements, and easily drill down into specific areas of interest.

Transactional analysis is one of the most powerful ways of detecting fraud within an organization. To maximize its effectiveness as a fraud detection system, the transactional analysis needs to:

- Allow easy comparisons of data and transactions from separate business or operational systems
- Work with a comprehensive set of indicators of potential fraud – taking into account the most common fraud schemes as well as those that relate specifically to the unique risks a particular organization may face
- Analyze all transactions within a given area and test them against the parameters that highlight indicators of fraud
- Perform the analyses and tests as close to the time of the transaction as possible, ideally even before the transaction has been finalized, and preferably on a continuous monitoring basis

Individuals intent on fraud seek out organizational “soft spots” where there is little regular cross-system data validation – they provide a golden opportunity for frauds to continue undetected.

This last point is of particular relevance. Many suspicious transactions or patterns only come to light when transactional data from one system is compared to that of another. In a simple example, this would involve comparing addresses of paid vendors with employee addresses, to detect potential “phantom vendor” schemes. Individuals intent on fraud seek out organizational “soft spots” where there is little regular cross-system data validation – they provide a golden opportunity for frauds to continue undetected.

Ad hoc, repetitive and continuous investigation

A fraud detection and prevention program should incorporate a spectrum of analysis – ranging from ad hoc through to repetitive through to continuous. Based on key risk indicators, ad hoc testing will pinpoint areas for further investigation. Should this initial testing reveal control weaknesses of suspected instances of fraud, repetitive testing or continuous analyses should be considered. Continuous review of internal controls is required to ensure that the controls that have been established remain in place and effective. In addition to having adequate controls, the challenge for auditors and fraud examiners is to look beyond the controls and find loopholes in the system where fraud could occur.

Benefits of using technology for effective fraud detection

A well-designed and implemented fraud detection system, based on transactional analysis of operational systems, can significantly reduce the chances of frauds occurring and then remaining undetected. The sooner indicators of fraud are available, the greater potential to recover losses and address any control weaknesses. The timely detection of fraud directly impacts the bottom line, reducing losses for an organization. And effective detection techniques serve as a deterrent to potential fraudsters; employees who know experts are present and looking for fraud are less likely to commit fraud because of a greater perceived likelihood they will be caught.

ACL enables timely fraud detection and prevention

ACL Services Ltd. is the leading global provider of technology for audit and compliance professionals. Combining market-leading audit analytics software and professional services expertise, ACL solutions give auditors confidence in the effectiveness of internal controls and the integrity of the transactions underlying business operations.

Since 1987, ACL has enabled auditors to assure sustainable compliance, reduce risk, detect fraud, enhance profitability, and improve business performance. ACL delivers its solutions to more than 215,000 licenced users in over 150 countries through a global network of ACL offices and channel partners. Our customers include 95 percent of Fortune 100 companies, 85 percent of the Fortune 500 and over two-thirds of the Global 500, as well as hundreds of national, state, and local governments, and the Big Four public accounting firms

ACL offers a series of white papers on specific Business Assurance issues. They define the challenges, examine solutions, and provide practical illustrations of the ways in which organizations have achieved business assurance in particular areas.

For a copy of the ACL white paper on which this summary is based (*Analyze Every Transaction in the Fight Against Fraud: Using Technology for Effective Fraud Detection*), please contact us at info@acl.com

» www.acl.com/frauddetection

■ acl.com
info@acl.com

ACL, the ACL logo, and Audit Command Language are trademarks or registered trademarks of ACL Services Ltd. All other trademarks are the property of their respective owners.

