WHITE PAPER

Analyze Every Transaction in the Fight Against Fraud:

Using Technology for Effective Fraud Detection

ACL™

Data you can trust. Results you can see.

CONTENTS

INTRODUCTION

Occupational fraud is a dominant form of white collar crime that exacts a significant toll on the organizations that fall prey to it, investors, financial institutions, as well as the overall economy. The Association of Certified Fraud Examiners estimates that a typical organization loses seven percent of its annual revenues as a result of occupational fraud and abuse.[1]

Fraud represents a significant business risk that must be mitigated. Effective fraud detection and prevention bolsters the bottom line by minimizing potential revenue leakage through unseen fraudulent activities. As compliance and standards initiatives such as the United States' Sarbanes-Oxley (SOX) Act and Statement and Auditing Standards (SAS) No. 99 create an increasingly more complex regulatory environment for organizations across the globe, demand has increased for greater scrutiny and visibility into the effectiveness of internal controls to minimize errors and reduce the opportunity for occupational fraud.

Finding fraud is an ongoing challenge that requires both skilled practitioners and specialized technology. There are several issues that make effective fraud management a particularly challenging task. These include: enormous and ever-expanding volumes of data; the growing complexity of systems; changes in business processes and activities; continuous evolution of newer fraud schemes to bypass existing detection techniques; false alarms; and regulatory issues related to employee privacy and discrimination.

This white paper focuses on the nature and scope of occupational fraud, and delves into solutions based on transactional data analysis.

THE NATURE OF FRAUD

In its *2008 Report to the Nation on Occupational Fraud and Abuse[1]*, the Association of Certified Fraud Examiners (ACFE) defines occupational fraud as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

Occupational fraud generally falls into three broad categories: asset misappropriations; corruption; and fraudulent financial statements. Asset misappropriations include revenue skimming, inventory theft, and payroll fraud. Common examples of corruption include accepting kickbacks and engaging in activities that represent a conflict of interests. Fraudulent statements generally involve falsifying an organization's financial statements by overstating revenues or understating liabilities and expenses.
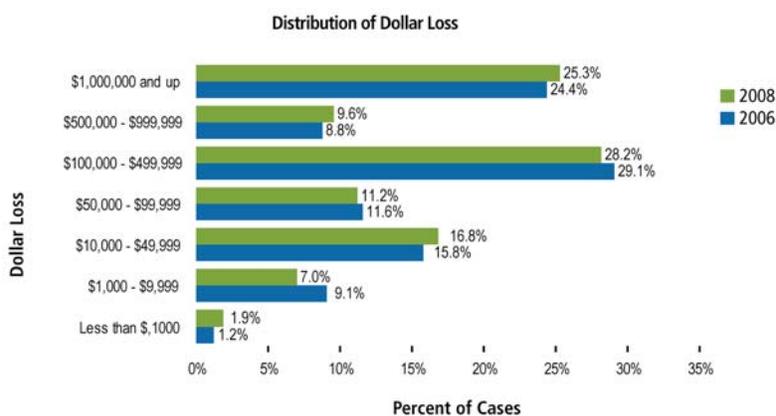
The vast majority of frauds surveyed in the ACFE 2008 study fell into the first category, "asset misappropriations", which occurred in nearly 90 percent of the cases reviewed and averaged a median loss of $150,000. Conversely, fraudulent statements were the least commonly reported fraud (about 10 percent), but had the highest median loss ($2 billion).[1] [All figures quoted in US dollars unless otherwise noted.]

---

[1] Association of Certified Fraud Examiners, *2008 Report to the Nation on Occupational Fraud and Abuse*.

The Extent and Costs of Occupational Fraud

The ACFE 2008 report estimates that a typical organization loses seven percent of its annual revenues as a result of occupational fraud and abuse. To illustrate the potential enormity of typical fraud loss, ACFE applied the seven percent figure to the estimated 2008 United States Gross Domestic Product — translating to about US $994 billion in fraud losses.[1]

The ACFE survey covered 959 occupational fraud cases – the median loss for all cases was US $175,000. More than 25 percent of the fraud cases caused losses of at least US $1 million, with 60 percent of fraud cases causing losses of at least $100,000. The median loss was greatest for Private Companies ($278,000) – who experienced over two and a half times the median loss impacting Government and Non-Profit ($100,000). [1]

Distribution of Dollar Loss

Dollar Loss	2008	2006
$1,000,000 and up	25.3%	24.4%
$500,000 - $999,999	9.6%	8.8%
$100,000 - $499,999	28.2%	29.1%
$50,000 - $99,999	11.2%	11.6%
$10,000 - $49,999	16.8%	15.8%
$1,000 - $9,999	7.0%	9.1%
Less than $,1000	1.9%	1.2%

Percent of Cases

Source: 2008 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

Diagram 1: Distribution of Dollar Losses

The losses are huge, and, according to a 2006 ACFE study, once the loss has occurred, the chance of recovering the funds in full is only 16.4 percent. Over 40 percent of survey respondents reported that they recovered nothing at all, and 23.4 percent were able to only recover one-quarter of their losses.[2] With billions of dollars funneling through the hands of fraudsters, the cost of timely detection or prevention of fraud is minimal when compared with the expense and effort expended to attempt recovery of lost funds.

Globally, fraud is taking its toll as well. Total reported fraud in the United Kingdom was £1.037bn in 2007 – not including a perceived growing number of unreported frauds.[3] In the Ernst & Young 9th Global Fraud Survey, one in five companies interviewed across 19 countries reported experiencing a significant fraud in the previous year.[4] When asked what factors were most likely to prevent or detect fraud, the majority of organizations surveyed in E&Y Survey stated that internal controls are generally the best-accepted manner in which to do so. However, the survey revealed, "For up to a quarter of companies'

---

[2] Association of Certified Fraud Examiners, *2006 Report to the Nation on Occupational Fraud and Abuse.*

[3] BDO Stoy Hayward, *FraudTrack 5: Fraud: A Global Challenge*, Annual Survey, 2008.

[4] Ernst & Young, *9th Global Fraud Survey: Fraud risk in emerging markets,* 2006.

foreign operations, the effectiveness of anti-fraud programs is limited by poor communication and/or insufficient training."[5]

In addition to the direct financial 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.

How Fraudsters Exploit Complex Systems

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.

Internal Controls Weaknesses

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.[6] Continuous review of internal controls is required to ensure that the controls that have been established remain in place and remain 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.

There are several issues that make effective fraud management a particularly challenging task. These include:

- Enormous and ever-expanding volumes of data

- The growing complexity of systems

- Changes in business processes and activities

- Continuous evolution of newer fraud schemes to bypass existing detection techniques

- False alarms

- Regulatory issues related to employee privacy and discrimination.

---

[5] Ernst & Young, *9th Global Fraud Survey: Fraud risk in emerging markets,* 2006

[6] KPMG Forensic, *Fraud Survey 2006: Fraud Risk Management.*

BUILDING A BETTER MOUSETRAP

Audit's Expanding Responsibility

The ACFE 2008 Report to the Nation found that "Internal Audit," "Internal Controls" and "External Audit" collectively account as the methods of initial detection in over 50 percent of fraud cases (19.4 percent, 23.3 percent and 9.1percent respectively). Organizations with the anti-fraud control of an Internal Audit/FE Department reduced their median loss to $118,000, compared to a median loss of $250,000 experienced by organizations without an Internal Audit function.[7]

The responsibility for fraud detection and prevention is shifting increasingly to internal audit departments, who have the skill set to provide real-time fraud risk assessment and monitoring and can report high-level and key risk area issues to management. PricewaterhouseCoopers's 2007 *Internal Audit 2012* survey reports that "Although antifraud roles vary in business today, top management generally owns the antifraud responsibility, the audit committee oversees antifraud efforts, and internal audit provides a critical line of defense against the threat of fraud by focusing on risk monitoring in addition to fraud prevention and detection."[8]

Strategize Your Fraud Detection Program

Instead of responding on a reactive basis to fraud within an organization, it's more effective to use strong internal controls and data analysis technologies to detect and, more importantly, prevent fraud from ever occurring in the first place.

Any complete fraud detection program must include the following steps:[9]

- **Build a profile of potential frauds.** This profile includes a list of the many different areas in which fraud may occur and the types of fraud that are possible in that area. This can be developed as part of a risk assessment.

- **Test transactional data for possible indicators of fraud.** A complete testing program should include ad hoc or random testing in addition to more formalized or regular tests. The spectrum of automated testing ranges from ad hoc through to repetitive through to continuous.

- **Improve controls by implementing continuous auditing and monitoring.** Strengthen controls over transaction authorizations and use continuous auditing and monitoring to test and validate the effectiveness of your controls.

- **Review information from data testing and continuous auditing and monitoring.** Investigate patterns and fraud indicators that emerge from the fraud detection tests and continuous auditing and monitoring.

- **Repeat the steps.** This process of building a profile, testing data, improving controls and reviewing information needs to be repeated on a regular basis.

- **Response.** Audit reports with recommendations on how to tighten controls or change processes to reduce the likelihood of recurrence.

---

[7] Association of Certified Fraud Examiners, *2008 Report to the Nation on Occupational Fraud and Abuse.*

[8] PricewaterhouseCoopers, *Internal Audit 2012: A study examining the future of internal auditing and the potential decline of a controls-centric approach,* 2007.

[9] ACL Services Ltd., *Using ACL to Detect Fraud: An ACL Workshop,* 2008

Controls Testing: Analyzing 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.

A fraud detection and prevention program should incorporate a spectrum of transactional data analysis — ranging from ad hoc to repetitive to continuous. Based on key risk indicators, ad hoc testing will pinpoint areas for further investigation. Should this initial testing reveal control weaknesses or suspected incidences of fraud, repetitive testing or continuous analysis should be considered. Transactional data analysis is one of the most powerful and effective ways of detecting fraud within an organization, and organizations can determine deployment along the analytics continuum based on the organization's transactional fraud risk areas. Transactional data analysis generally includes a comprehensive series of tests designed to detect indicators of a wide range of frauds. To maximize its effectiveness as a fraud detection system, transactional data analysis ideally will:

- Allow easy comparisons of data and transactions from multiple IT systems

- Work with a comprehensive set of indicators of potential fraud – taking into account both the most common fraud schemes and 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 continual basis.

Despite the numerous benefits, many organizations only use such techniques on an occasional test basis, and often only in a reactive fashion, once a problem is suspected. In many cases, the tests performed are fairly simplistic and are unlikely to uncover more sophisticated frauds. The full power of data analysis technology has yet to be exploited by many organizations.

KPMG Forensics' 2006 Fraud Risk Management report found that "Unlike retrospective analyses, continuous transaction monitoring allows an organization to identify potentially fraudulent transactions on, for example, a daily, weekly or monthly basis. Organizations frequently use continuous monitoring efforts to focus on narrow bands of transactions or areas that pose particularly strong risks."[10] By continuously auditing and monitoring operational data and transactions, organizations can catch frauds earlier in the fraud cycle – preventing greater losses, and quite often serving as a deterrent to other possible frauds.

Analytic Techniques for Fraud Detection

A number of specific analysis techniques have proven effectiveness in detecting fraud:

- Calculation of statistical parameters such as averages, standard deviations, and highest and lowest values to identify statistical anomalies

- Classifications to find patterns and associations among groups of data

- Stratifications of numeric values to identify unusual and outlying values

- Digital analysis, using Benford's Law, to identify statistically unlikely occurrences of numeric amounts

---

[10] KPMG Forensic, *Fraud Survey 2006: Fraud Risk Management.*

- Joining or matching data fields between disparate systems, typically looking for expected matches or differences for data such as name, address, telephone, or part/serial number

- "Sounds like" functions that identify fraudulent variations of valid company and employee names

- Duplicates testing that identifies both simple or complex combinations of duplication

- Gaps testing that identifies missing sequential data

- Summing and totaling to check control totals that may be falsified

- Graphing to provide visual identification of anomalous transactions

Typical Types of Fraud and Fraud Tests

Knowing what to look for is critical in building a fraud detection program. The following examples are based on descriptions of various types of fraud and the tests used to discover the fraud as found in *Fraud Detection: Using Data Analysis Techniques to Detect Fraud*.[11]

Type of Fraud	Tests Used to Discover This Fraud
Fictitious vendors	- Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers - Be alert for vendors with similar sounding names or more than one vendor with the same address and phone number
Altered invoices	- Search for duplicates - Check for invoice amounts not matching contracts or purchase order amounts
Fixed bidding	- Summarize contract amount by vendor and compare vendor summaries for several years to determine if a single vendor is winning most bids - Calculate days between close for bids and contract submission date by vendor to see if the last bidder consistently wins the contract
Goods not received	- Search for purchase quantities that do not agree with contract quantities - Check if inventory levels are changing appropriate to supposed delivery of goods
Duplicate invoices	Review for duplicate invoice numbers, duplicate date, and invoice amounts
Inflated prices	Compare prices across vendors to see if prices from a particular vendor are unreasonably high
Excess quantities purchased	- Review for unexplained increases in inventory - Determine if purchase quantities of raw materials are appropriate for production level - Check to see if increases in quantities ordered compare similarly to previous contracts or years or when compared to other plants
Duplicate payments	- Search for identical invoice numbers and payments amounts - Check for repeated requests for refunds for invoices paid twice
Carbon copies	Search for duplicates within all company checks cashed; conduct a second search for gaps in check numbers
Duplicate serial numbers	Determine if high value equipment a company already owns is being repurchased by checking serial numbers for duplicates and involvement of same personnel in purchasing and shipping processes
Payroll fraud	Find out if a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck and extract all pay transactions for departure date less than date of current pay period
Accounts payable	Reveal transactions not matching contract amounts by linking Accounts Payable files to contract and inventory files and examining contract date, price, ordered quantity, inventory receipt quantity, invoice quantity, and payment amount by contract

---

[11] Coderre, David G., *Fraud Detection: Using Data Analysis to Detect Fraud, 2nd edition* (Vancouver, BC: Ekaros, 2004)

Application Areas for Transactional Data Analysis

Enterprising fraudsters can and will exploit weakness wherever they find it. Computerized transactional data analysis has proven itself a reliable aid in fraud detection in a wide range of business processes, including:

- Accounts Payable
- Accounts Receivable
- Bid Rigging
- Cash Disbursements
- Conflict of Interest
- Credit Card Management
- Customer Service Management
- Deposits

- General Ledger
- Kickbacks
- Life Insurance
- Loans
- Materials Management and Inventory Control
- Policy and Administration
- Purchase Order Management

- Real Estate Loans
- Retail Loss Prevention
- Salaries and Payroll
- Sales Analysis
- Travel Claims
- Vendor Management
- Work In Progress

TIMELY FRAUD DETECTION USING *ACL*

The ACL approach to fraud detection is based on comprehensive analysis of the transactional data flowing through financial and operational systems. Using ACL technology to access and analyze unlimited volumes of data from virtually any enterprise application, organizations can quickly identify suspicious transactions that may represent fraud, error, and abuse, and close control loopholes before fraud escalates. ACL provides an integrated, cost-effective set of technology that may be flexibly deployed along the full audit analytics continuum based on an organization's needs and fraud risk areas. ACL audit analytics technology supports exploratory ad hoc investigations – the kind typically undertaken by skilled auditors or fraud investigators – and also supports the embedding of automated, pre-defined analytics within the core business processes that represent high-risk areas to the organization for sustainable, scalable, immediate and continuous analysis.

Audit analytics in action: case study

The Austrian Ministry of Finance has an annual budget of over €110 billion per year and is responsible for the coordination of taxation and customs programs throughout Austria. The Ministry auditors must analyze enormous quantities of data from a wide variety of computer platforms, while operating under acute time pressures. In Austria, all companies and individuals must submit their tax data electronically, but are allowed to do so in many formats.

ACL's flexible audit analytics software has been key to the Ministry's ability to improve the scope and effectiveness of its tax audits. In one major initiative, over a four-year period, the Electronic Data Processing (EDP) audit team used powerful audit analytics to identify, and then recover, €85 million in missed tax revenues – and was able to stop a fraud scheme that had been exploited by the hospitality sector for years.

Benefits of ACL Audit Analytics Technology

ACL's robust analytics technology enables analysis of even the largest volumes of transactional data in a fraction of the time once required, so that all pertinent data from any number of systems can be quickly analyzed for flagging potential indicators of fraud.

Through a unique and powerful combination of data access, analysis, and integrated reporting capabilities, ACL software reaches data from virtually any source, across any system, through a consistent user interface – whether housed in mainframes, servers, legacy systems, or PC networks. By independently comparing and analyzing data from ERP, CRM, SCM, or other enterprise applications,

ACL technology enables immediate insight into the transactional data underlying core business processes and financial reporting.

In the most recently conducted IIA *Internal Auditor* software survey (2006), ACL was selected by 35 percent of the participants as the tool of choice for fraud prevention and detection.

Fraud Detection/Prevention Software
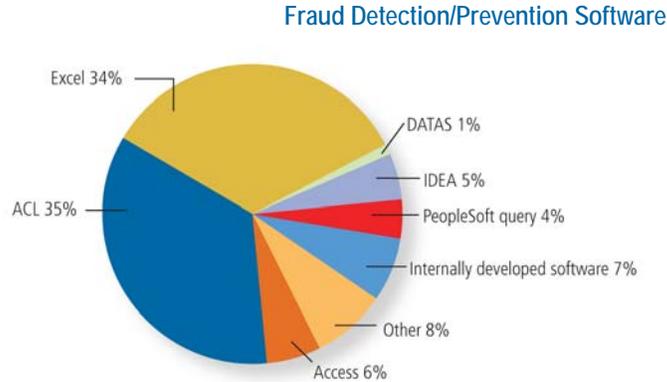
Reprinted with permission from *Internal Auditor* (August 2006), published by The Institute of Internal Auditors, Inc. www.theiia.org

Audit analytics in action: case study

Forensic accounting and fraud examination specialists, Forensic Strategic Solutions PC, were hired by the Los Angeles Unified School District (LAUSD) to perform an examination of the District's Belmont Learning Complex project. Mired with problems and a price tag estimated at over $200 million, the construction project for the high school became the most expensive in the country before the District was forced to step in and stop construction. Using ACL audit analytics technology, Forensic Strategic Solutions investigative audit uncovered:

- 48 budget transfers authorized by one employee for $49,999 each within a four-month period circumventing LAUSD's policy requiring that any spending greater than $50,000 receive approval from the Board of Education

- Overbilling of $2.1 million through payment applications made by the project developer, construction contractor, and some of the sub-contractors

- Circumvention of the proper payment codes using direct payments, resulting in outstanding encumbrances over a period of five fiscal years totaling approximately $77.8 million

ACL for Fast Implementation and Fast Payback

The ease and speed of implementing a complete ACL solution means not only more timely detection of fraud and faster return on investment, but also more effective, systematic fraud prevention over the long term. Having an effective system for fraud prevention in place is part of business assurance – the knowledge that an organization can rely on the accuracy, reliability, and integrity of all its data and transactions to make decisions with speed and confidence. ACL solutions provide audit, compliance, and financial professionals with the confidence that they are seeing the full picture – giving clients the ability to find fraud, stop overpayments, and improve operational efficiency.

ACL technology enables access to corporate data sources by allowing efficient processing of unlimited data populations and cross-platform data analysis. ACL enables effective management and security of data and results by allowing centralized access to data on a server that does not require duplication of data to local machines. This also supports increased collaboration by having data available for analysis by multiple team members. Automation of fraud tests with ACL enables coverage of 100% of transactions to increase confidence in results, and frees staff time from data analysis to permit a fast response in investigating identified breaches.

CONCLUSION

Fraud is a significant business risk that must be mitigated. A well-designed and implemented fraud detection system, based on the transactional data analysis of operational systems, can significantly reduce the chance of fraud occurring within an organization. The sooner that indicators of fraud are available, the greater the chance that losses can be recovered and control weaknesses can be addressed. 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 that experts are present and looking for fraud or that continuous monitoring is occurring are less likely to commit fraud because of a greater perceived likelihood that they will be caught.

Given increased regulatory requirements and compliance demands, the decision is no longer if an organization should implement a complete fraud detection and prevention program, but rather how quickly that program can be put into place. The use of technology is essential for maximizing the efficiency and effectiveness of a fraud detection and prevention program.

To find out how ACL can help your organization combat fraud, contact us at **+1-604-669-4225** or **info@acl.com** to arrange for a free consultation.

COMPANY OVERVIEW

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.

ACL Headquarters

T +1 604 669 4225
F +1 604 669 3557

■ acl.com
info@acl.com

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 licensed 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. www.acl.com