

# Prodigy Newsbyte

Issue 2

Feb to Apr 2003

## Special points of interest:

- How much is your organization losing to undetected Fraud?
- Six Steps of Detecting Fraud
- ACL Tips of the Month - Detecting Corporate Credit Card Abuse!
- ACL User Feature
- Specialised Training: Fraud Detection Techniques Using ACL
- Special Indonesia Training Rates

## Inside this issue:

Building a better mousetrap thru': Transactional Analysis & Continuous Monitoring	2
ACL Tips of the Month	2
On a Lighter Side	2
Using ACL to Monitor Fraud	3
Specialised Training: Fraud Detection Techniques Using ACL	3
Special Indonesia Training Rates	4
ACL Training Schedule	4

## How much is your organization losing to undetected fraud?

The Association of Certified Fraud Examiners (ACFE) estimates that six percent of organizations' revenues will be lost this year as a result of occupational fraud. Within the United States, this translates into losses of approximately \$600 billion or about \$4,500 per employee. The ACFE's 2002 Report to the Nation on Occupational Fraud and Abuse covered 663 occupational fraud cases that caused more than \$7 billion in losses. More than half of the frauds in this study involved losses of at least \$100,000 and nearly one in six 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.

In simple terms, frauds fall into three broad categories: asset misappropriation, corruption or fraudulent statements. Based on the ACFE study, over 85 percent of the occupational frauds reviewed involved asset misappropriation, with cash as the targeted asset 90 percent of the time. Corruption schemes accounted for nearly 13

percent of frauds studied, for an average loss of more than \$500,000 per incident. Organizations traditionally have looked to prevent and detect fraud by implementing appropriate internal controls. Internal audit typically tests and validates these controls during regular audit processes - uncovering 18 percent of frauds detected according to the ACFE study - but the role is essentially reactive. Internal controls and external audit are responsible for uncovering a further 30 percent of detected fraud, but the balance of cases - in fact the majority - come to light through tips or accident.

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. The ACFE study found that 46 percent of detected frauds occurred because of insufficient number of frauds are simply never detected.

Even when fraud 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.

## The Six Steps of Detecting Fraud

1. Determine the organization's risk of fraud by developing an understanding of the operational and control environments
2. Develop a thorough understanding of the symptoms of fraud
3. Develop an alertness to the occurrence of the symptoms of fraud
4. Develop programs to look for the symptoms of fraud
5. Investigate and report instances of fraud
6. Design and implement controls to deter the recurrence of fraudulent activity



## ACL Tips of the Month - Detecting Corporate Credit Card Abuse!

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.

## Building a better mousetrap through: Transactional Analysis and Continuous Monitoring

Both the Association of Certified Fraud Examiners and the American Institute of Certified Public Accounts refer specifically to the use of computerized analysis to assist in fraud detection techniques. Such analyses are particularly effective in detecting frauds that fall into the most common fraud categories—asset misappropriation and fraudulent disbursements.

Both professional associations detail indicators of the most types of fraud and cite examples of the kinds of analyses that can be performed to detect them. However, many organizations use such techniques on an occasional test basis and often only in reaction to suspected problems. In many cases, the tests performed are fairly simplistic and are unlikely to uncover more sophisticated fraud schemes.

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 need to:

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.

- ◆ Analyse 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

- ◆ Allow easy comparisons of data and transactions from separate business or operational systems

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, 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.

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.



## On A Lighter Side



Copyright © 2002 United Feature Syndicate, Inc.

## Using ACL to Monitor Fraud

Several major issues confronting companies in today's business is fraud. Some of the frauds are unable to be detected due to several reasons. Therefore, it is imperative for companies to examine their exposures and to provide an effective way to manage these liabilities.

One example is that the more a consumer shops online or non-online, the more he is exposed to hacking and misuse. Fraud is a problem that has grown dramatically over the past years.

The advancement of technology has been largely beneficial to operators and customers processes become quicker and smoother. Hence, hardware becomes

cheaper and great cost savings can be made.

However, along with all the benefits there are also downsides and danger. One of the main problems with technology, has been the advancement of fraud. As soon as the operators find ways to stop one type of fraud, another is created. One common limitation that companies encounter is time constraint and poor method in detecting the frauds.

Seeking expertise from proven software like ACL is an essential move. I have personally have used ACL software, it is so effective and fast in detecting fraud activities which cannot be seen by an ordinary person. It gives 100% data satisfaction

and confident to all functions in an organization.



*Dr Bala Sekar nadarajan (PhD) from Malaysia has held several corporate posi-*

*tions and worked with several global consulting firms. He was responsible for developing several big large companies risk management, corporate governance, fraud detection, internal controls, business improvement, TQM frameworks and etc. Currently, he is the CEO of Smart Business Consulting and also heads the Malaysian Professional Networking group which consist of Directors/CEO/Auditors and other professionals.*

### ACL Specialised Training: Fraud Detection Techniques Using ACL

In this 2-day session, participants will gain further insight on the most efficient and effective techniques of using ACL for Windows to detect fraud. ACL users should leave the course with the skills to combat against abuse and fraud.

The professionals for whom this course has been developed need to have a knowledge of standard Windows operations (opening/closing files, navigation). Participants must have a fundamental understanding of ACL for Windows by attending Introductory ACL for Windows training.

You will learn...

- ◆ **Basic Concepts of Fraud**
- ◆ **Fraud Schemes**
- ◆ **Fraud Detection Techniques**

**12-13 May 2003  
Singapore**

We urge you to sign up early to confirm your enrolment. For more information, please contact us at +65 6221-2810 or [info@prodigy.com.sg](mailto:info@prodigy.com.sg)

Are you getting the most out of data analysis software? Prodigy Data Solution can help you acquire the skills you need to realize the full value of ACL

PRODIGY DATA SOLUTION  
PTE LTD

201B NEW BRIDGE ROAD  
SINGAPORE 059428  
TEL: (65) 6221 2810  
FAX: (65) 6221 2813  
EMAIL:  
[INFO@PRODIGY.COM.SG](mailto:INFO@PRODIGY.COM.SG)

PRODIGY DATA SOLUTION  
PTE LTD

201B NEW BRIDGE ROAD  
SINGAPORE 059428  
TEL: (65) 6221 2810  
FAX: (65) 6221 2813  
EMAIL:  
INFO@PRODIGY.COM.SG

visit us at  
[www.prodigy.com.sg](http://www.prodigy.com.sg)

Coming Up in the  
Next Issue of Prodigy  
Newsbyte

- ◆ More Useful ACL Tips
- ◆ Articles on Risk Management
- ◆ ACL User Feature
- ◆ And many other useful industries information

Feel free to write us  
any questions,  
comments or  
feedbacks on Prodigy  
Newsbyte via email at  
[info@prodigy.com.sg](mailto:info@prodigy.com.sg)

## ACL FOR WINDOWS TRAINING IN INDONESIA

### Special Indonesia Rate

	Open Enrolment	On-Site	Duration
	Per Participant (US\$)	Per Class (US\$)	
ACL – Introductory	\$ 333	\$ 3,000	3 days
ACL – Intermediate Workshop	\$ 278	\$ 2,500	2 days
ACL – Developing Applications	\$ 333	\$ 3,000	2 days
ACL – Functions	\$ 167	\$ 1,500	1 day
ACL – Data Access	\$ 167	\$ 1,500	1 day
ACL – Refresher	\$ 167	\$ 1,500	1 day

### Indonesia Open Enrolment Training Schedule — Feb to Apr 2003

COURSE NAME	DATES
ACL for Windows - Introductory	February 18 to 20; 25 to 27
	March 5 to 7; 11 to 13; 17 to 19
	April 7 to 9; 15 to 17; 21 to 23; 28 to 30
ACL for Windows - Intermediate Workshop	April 3 to 4
ACL for Windows - Data Access	February 21; 28
	March 21; 31
	April 14
ACL for Windows - Refresher	March 3; 10; 24
	April 1; 25
ACL for Windows - Functions	April 11

### ACL Open Enrolment Training Schedule — Feb to Apr 2003

VENUE	COURSE NAME	MONTH	DAY
Singapore	ACL for windows - Introductory	February	05 - 07
		March	10 - 12
		April	01 - 03
	ACL for windows - Intermediate Workshop	February	20 - 21
		April	14 - 15
	ACL for windows - Data Access	April	16
	ACL for windows - Functions	April	17
	ACL for windows - Developing Applications	March	13 - 14
ACL for windows - Refresher	April	18	
Kuala Lumpur, Malaysia	ACL for windows - Introductory	February	04 - 06
			17 - 19
		March	04 - 06
			18 - 20
	April	07 - 09	
		28 - 30	
	ACL for windows - Intermediate Workshop	April	10 - 11
	ACL for windows - Data Access	March	21
April		17	
ACL for windows - Developing Applications	March	06 - 07	
Bangkok, Thailand	ACL for windows - Introductory	March	24 - 26
	ACL for windows - Developing Applications	March	27 - 28
India	ACL for windows - Introductory	April	21 - 23
	ACL for windows - Developing Applications	April	24 - 25
Philippines	ACL for windows - Introductory	February	24 - 26
	ACL for windows - Intermediate Workshop	February	27 - 28

For training dates beyond April 2003, please contact us at [info@prodigy.com.sg](mailto:info@prodigy.com.sg)