Paper 158-2008

Technology Solutions to Detect Fraud

Author, Eckhardt Kriel, E Kriel & Associates, Oakville, ONTARIO

ABSTRACT

This paper discuses the use of technology in the area of fraud detection. Using a number of case studies Eckhardt will discuss various techniques and technology solutions which he has used in the past.

It is intended for:

- management, who has an obligation to certify financial information and the effectiveness of internal control over financial reporting or who has to meet other compliance or operational requirements and;
- auditors and investigators charged with the audits of financial information, value for money audits or forensic investigations.

Since the collapse of Enron on December 2, 2001 and other corporate failures around the world, wide-ranging changes have been made to the regulatory environment of business. Corporate governance has become a common focus for many boards and audit committees.

In an attempt to restore confidence in the markets, securities regulators have promulgated various pieces of legislation, namely the Sarbanes-Oxley Act of 2002 in the US and Bill 198 and Multilateral Instrument 52-109 in Canada that require the certification of the design and the effectiveness of internal control over financial reporting by the CEO and CFO.

Perhaps one of the more far-reaching revisions to the auditing standards concerns the auditor's responsibility to consider fraud. In all of these new standards and guidelines, technology solutions can play an ever-increasing role to the point where their use is now becoming a necessity, especially in the area of fraud detection.

INTRODUCTION

This paper will not cover all the technical solutions to detect and prevent fraud as there are a multitude of them. Rather it focuses on an approach that attempts to address the shortcomings in previous attempts by auditors and investigators who are trained in traditional accounting and auditing methods. Since the collapse of Enron on December 2, 2001 and other corporate failures around the world, wide-ranging changes have been made to the regulatory environment of business. Corporate governance has become a common focus for many boards and audit committees.

In an attempt to restore confidence in the markets, securities regulators have promulgated various pieces of legislation, namely the Sarbanes-Oxley Act of 2002 in the US and Bill 198 and Multilateral Instrument 52-109 in Canada that require the certification of the design and the effectiveness of internal control over financial reporting by the CEO and CFO.

Perhaps one of the more far-reaching revisions to the auditing standards concerns the auditor's responsibility to consider fraud, especially in SAS 99. In all of these new standards and guidelines, technology solutions can play an ever-increasing role to the point where their use is now becoming a necessity, especially in the area of fraud detection.

The PricewaterhouseCoopers' 2007 Global Economic Crime Survey[1] contains startling statistics that reveal that fraud is not going away and is a global phenomenon despite the implementation of SOX for number of years. An interesting observation is made that a possible reason for the increase in fraud since 2003 is that the implementation of SOX has made the detection of fraud more common.

WHY TRADITIONAL METHODS OFTEN FAIL

Fraud is based on deception – you are not supposed to find it. Even if you are looking for it, it can be hard to find.

Auditors have traditionally been trained to find evidence to support a premise that assertions embodied in financial statements are right. When suspicious circumstances exist the initial premise must change to the premise that they might be wrong – it requires a switch.

Until recently auditors have been limited by standards that have enshrined a tenet of reliance on the presumption of management's good faith.

Audit processes designed to detect such fraud remain problematic because there is no deployed body of knowledge among auditors about what fraud looks like. If faced with a suspicion that there might be needles in the haystack, an auditor might be tempted to sample the hay to support a conclusion that the hay is what it is purported to be, with sampling precision. A fraud investigator would shift the focus to the needles and knowing what the needles look like would be crucial to the investigation.

Asset Misappropriation Fraud

Traditional methods of detecting fraud using data analysis techniques have failed largely because auditors have not known what to look for. The traditional inductive approach allowed them to detect a small number of frauds. For example, in the case below, which is based on an actual fraud case, it is relatively easy to spot the fraudulent expense claims:

[1] (PricewaterhouseCoopers, 2007)

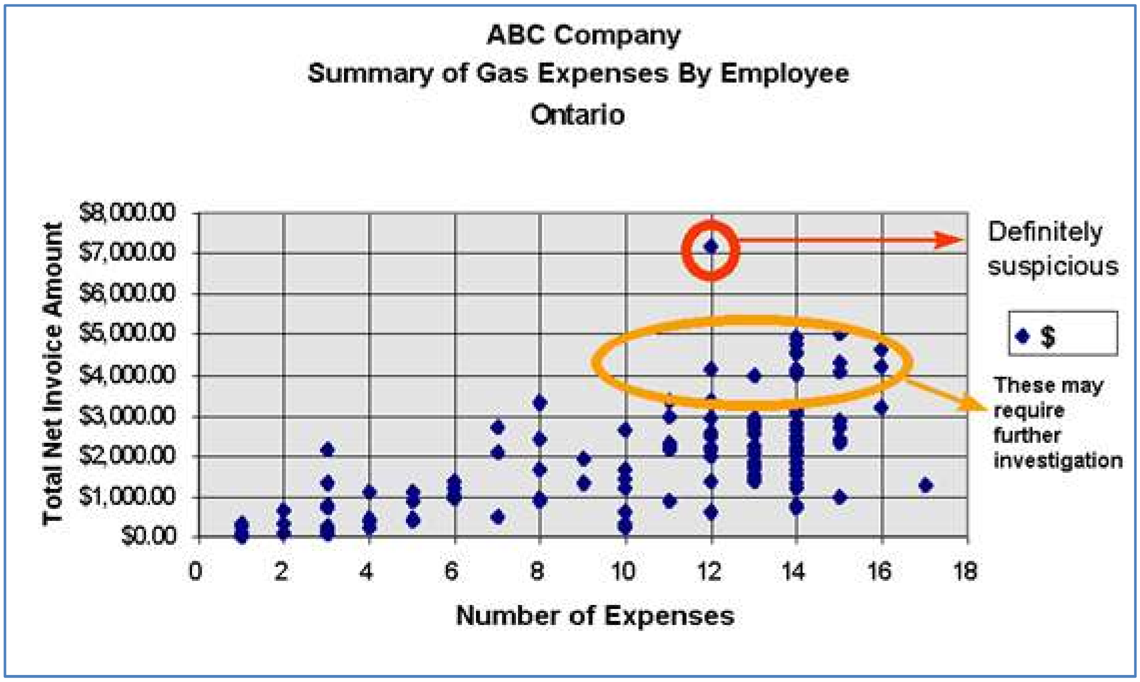


Figure 1 Fraudulent expense claim

However, this approach presents a number of weaknesses. In the case above (Figure 1), the perpetrator was foolish enough not to hide the fraudulent claims, making the claims totalling $7,185 easy enough to spot. But what of the fraudster who deliberately conceals the fraudulent claims? A fundamental rule of fraud from the perpetrator's point of view is "cover your tracks," so even if the auditor is looking for fraud, it can be hard to find.

The attempt at deception is what distinguishes fraud from error, posing challenges as regards both detection and risk management. These challenges invite some simple but compelling responses:

- "If you want to find fraud, you have to know what it looks like."
- "If you want to prevent fraud, you have to know what causes it."
- "There is always evidence of fraud when it occurs."
- "The real numbers always exist."[2]

Traditionally fraud investigations have usually begun with anonymous tips, financial reporting anomalies, or errors that have led to system overrides. These indicators, often called red flags, provide clues that fraud might exist in an organization.

Auditors follow up on these indicators with interviews, additional research, computer interrogations and document reviews, to determine if fraud exists and its real cause. This approach can be viewed as an inductive method: it begins

[2] (Hodson N. M., 2004; Hodson N. M., 2007)

with specific indications of fraud and continues by investigating reports, documents and data until the general type of fraud is identified.

Technology can make it possible to reverse this approach. The auditor can start with general or common fraud types and determine whether the indicators exist. The auditor develops a hypothesis of a fraud that might exist and formulates the characteristics of what the data might look like if that fraud actually happened.

I call this method the deductive method of fraud detection — starting with general fraud types and moving forward to determine whether indicators or red flags of those frauds exist. Using data analysis techniques the auditor can target different types of frauds, analyze entire populations, and zero in on fraud before traditional indicators appear. My presentation will outline this in more detail and cover this in a case study.

An example of a deductive approach is to consider accounts payable and payments, one of the most common frauds is the payment of invoices to fictitious suppliers. In order to identify fictitious suppliers on the vendor master file, the auditor has to formulate a hypothesis of what constitutes a fictitious supplier and what it would look like if it were to appear in the vendor master file.

After giving the matter some careful thought, the auditor would likely establish the following criteria:

- A fictitious supplier would only be used by one person in the organization.
- The invoices from a fictitious supplier would all be in numerical sequence, as this supplier would have no other customers.
- The amounts invoiced from this supplier would be big enough to make it worthwhile for the perpetrator of the fraud, yet small enough to escape detection through a routine audit.
- Transactions with the fictitious supplier would be completed rapidly, from the time the order was placed or the invoice received to the time the cheque was issued, to decrease the risk of detection.
- Since there would never be a dispute with a fictitious supplier, there would never be credit memos in the account.
- The name of the fictitious supplier would probably not contain the names or parts of names of established organizations like Bank, Insurance, etc.
- The name of the fictitious supplier would likely consist of initials and the words “consultants,” “services,” etc.
- The address of the fictitious supplier would probably not be a real address but a P.O. Box number or similar.

Additional criteria could be established, but these serve as an example. This technique for detecting fraud could be applied to other audits and will most often be successful if the criteria are developed in cooperation with an experienced forensic accountant. These criteria are sometimes referred to by the fraudsters themselves. For example, in a recent television interview Mark Morze of ZZZZ Best said:

‘I created over 10,000 false documents… My suppliers were all false, phony PO Box numbers, phony addresses… If only the auditors had called a supplier I would have been sunk.” [3]

[3] (Morze, 1994)

FINANCIAL REPORTING FRAUD

A review of the circumstances leading to the frauds perpetrated in the past few years by companies such as Enron, Cendant, WorldCom and HealthSouth, to name but a few, shows that they involved the deliberate manipulation of financial reports. The perpetrators used false entries including fraudulent journal entries in a variety of schemes to manipulate revenue and earnings, to falsely capitalize expense items as assets, to conceal liabilities and to tamper with reserves.

Statement of Auditing Standard 99 –indicates certain matters the auditor would consider for the purposes of identifying and selecting journal entries and other adjustments for testing, and also details the characteristics of fraudulent journal entries or other adjustments. Such characteristics may include entries:

- made to unrelated, unusual or seldom-used accounts;
- made by individuals who typically do not make journal entries;
- recorded at the end of the period or as post-closing entries that have little or no explanation or description;
- made either before or during the preparation of the financial statements that do not have account numbers; or
- containing round numbers or consistent ending numbers.

In a large company, many hundreds of thousands of journal entries can be made every year and it is difficult to imagine how an audit can be conducted effectively using a manual review of all entries or even a statistical sample.

With technology, the auditor can design a range of tests, including tests to identify the characteristics noted above.

EXAMPLES OF TECHNICAL TOOLS AND TECHNIQUES

David G. Coderre[4] has produced a Fraud Toolkit for ACL which performs a range of tests on data files from various business processes, e.g., Sales, Purchases, Inventory, payroll, etc. The Toolkit contains example code as well as a CD-ROM disk with sample code.

Also auditors have used analytical tools for the following substantive type tests:

- Extract
- Sample
- Summarize
- Total, count
- Classify
- Sort
- Re-calculate
- Compare
- Stratify
- Merge, split and join
- Calculate ratios
- Test sequences, for duplicates, and gaps
- Test aging calculations
- Print confirmations
- Produce graphs and charts

[4] Coderre David, G: Fraud Toolkit for ACL, Global Audit Publications, 2001

I cannot cover all of these in this presentation but mention several below briefly.

Example of Analysis of Outliers

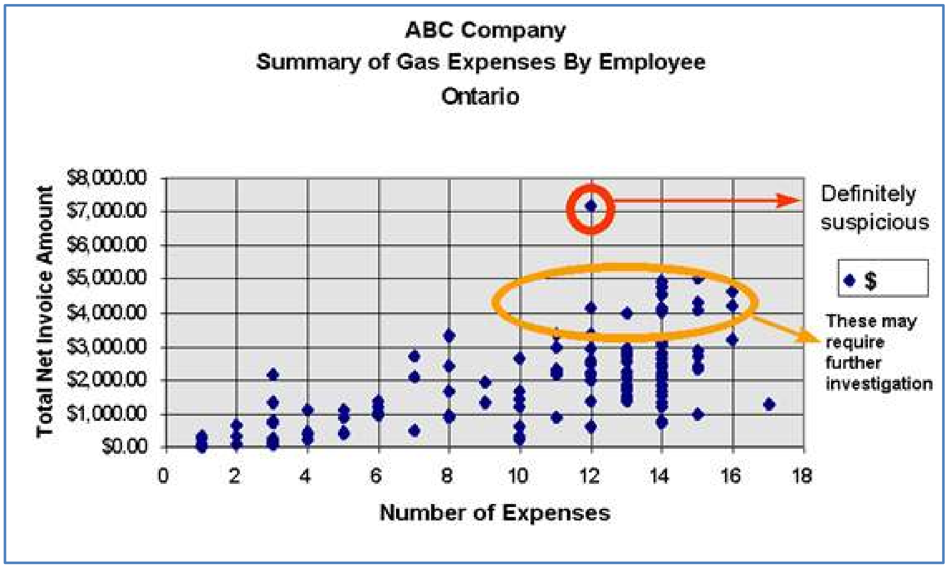


Figure 2 Example of fraud outlier

Using techniques like histograms and frequency charts an auditor can easily examine a large data set for unusual amounts and plot them in a graphical manner which is easy to interpret as can be seen in Figure 2 above.

Benford's Law

Most people would think that in a random sample of digits the digits 1 to 9 would each occur with an equal probability. In1938 Frank Benford published his "Law of Anomalous Numbers" paper that presented the digit patterns expected in natural data sets and he found that the digit patterns are counter intuitive because the low digits are assigned higher probabilities of occurring than the higher digits. The digit patterns have been reviewed and discussed in more than 100 academic papers; notably a paper in 2004 By Cindy Durtschi, William Hillson and Carl Pacini entitled: **"The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data**." [5]

The digit patterns can be calculated using the following formula: LOG(1 +(1/n)) where n=digit. On a spreadsheet this can be displayed as follows:

Digit	Probability
1	30.10299957%
2	17.60912591%
3	12.49387366%
4	9.69100130%
5	7.91812460%
6	6.69467896%
7	5.79919470%
8	5.11525224%
9	4.57574906%
Total	100.00000000%

[5] (Durtschi, Hillson, & Pacini, 2004)

When plotted on a graph one gets a plot which conforms to a so-called Benford Set. See Figure 3 below.

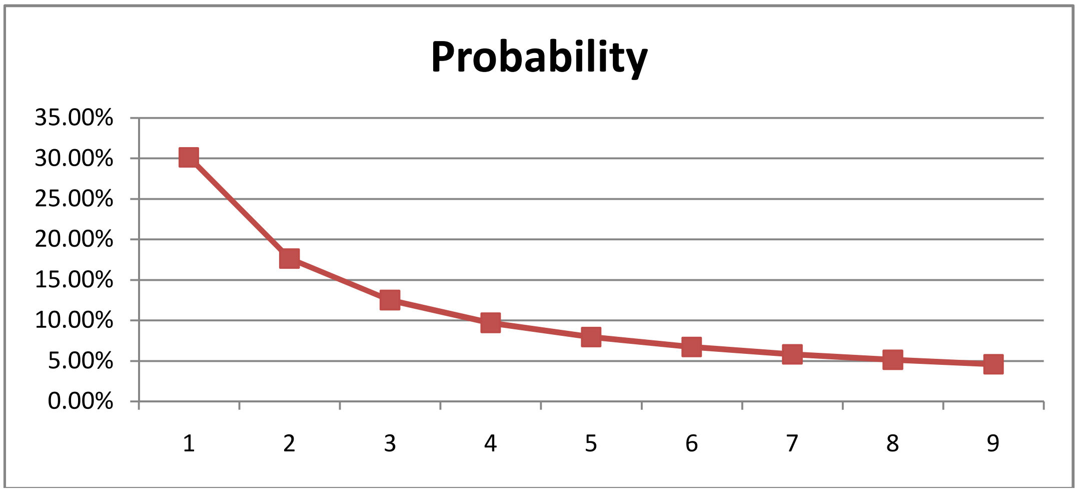


Figure 3 Plot of digit frequencies

Dr. Mark Nigrini gained recognition a few years ago by applying a system he devised based on Benford's Law to some fraud cases in Brooklyn, N.Y. The idea underlying his system is that if the numbers in a set of data like a tax return more or less match the frequencies and ratios predicted by Benford's Law, the data are probably honest. If a graph of such numbers is markedly different from the one predicted by Benford's Law, it might indicate errors or fraudulent activity.

Benford's Law has been extended to show that the first two digits (also trailing digits) of certain data sets demonstrate similar characteristics that enable numerical discrepancies to be identified. The chart below (Figure 4) shows an acceptable plot of numbers that conform to Benford’s Law. This called the First Order Test.

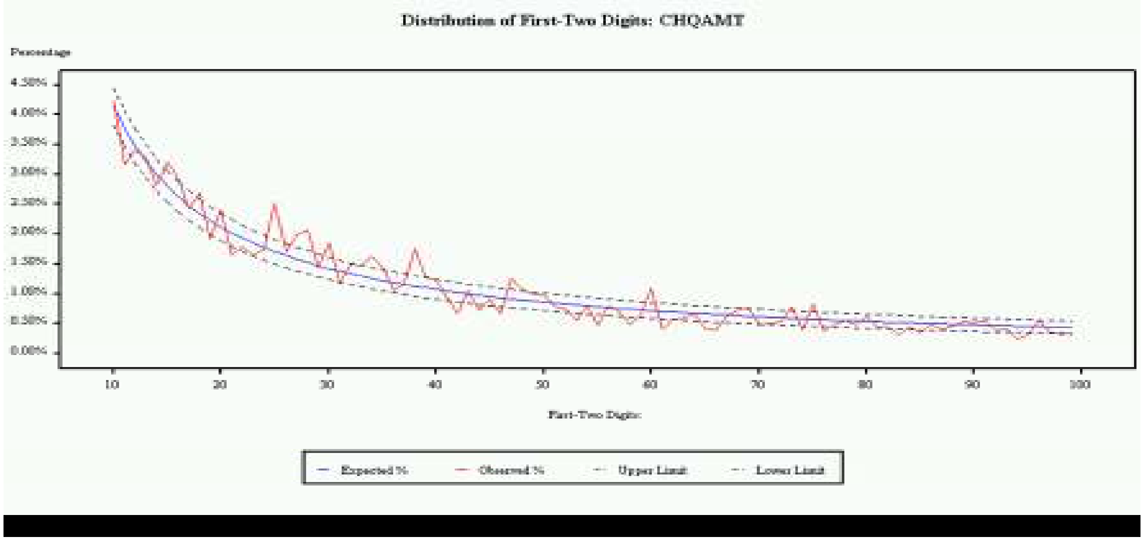
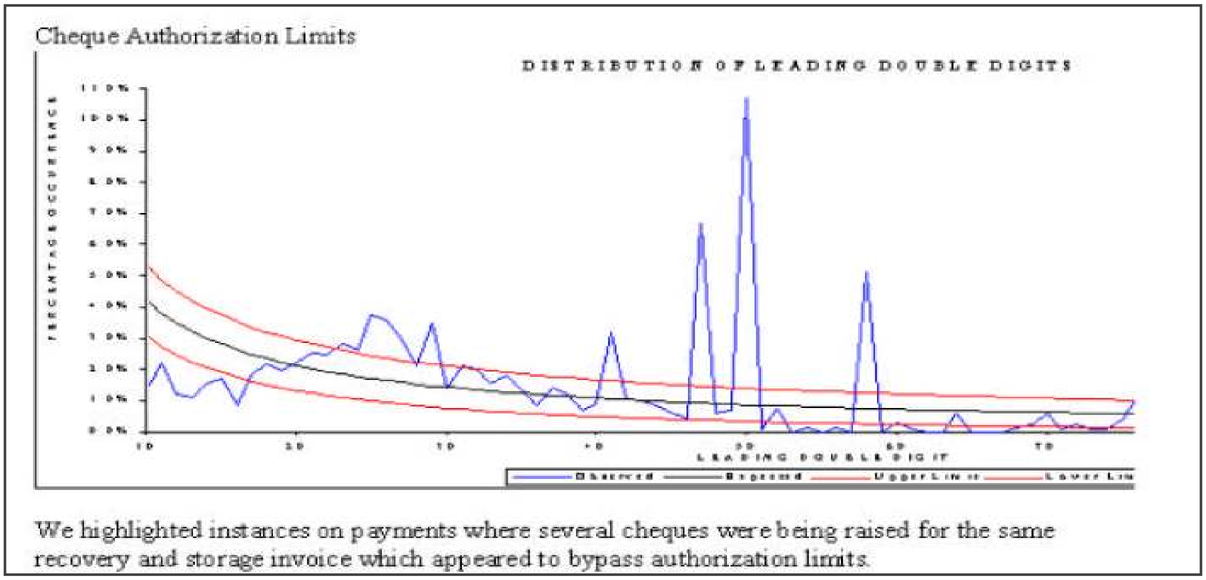


Figure 4 Standard Benford curve

The diagram below (Figure 5) depicts an instance of check fraud and the peaks show cases where checks were written just below authorization limits



We highlighted instances on payments where several cheques were being raised for the same recovery and storage invoice which appeared to bypass authorization limits.

Figure 5 Fraud shown in Benford curve

Second Order Benford Tests

Recently Dr. Mark Nigrini and Dr. Steven Miller published a paper called "DATA DIAGNOSTICS USING SECOND ORDER TESTS OF BENFORD'S LAW".[6] In the paper the authors describe a new second-order test that is an analysis of the digit frequencies of the differences between the ordered (ranked) values in a data set. These digit frequencies approximate the frequencies of Benford's Law for most data sets. The second-order test can be applied to any data. The test generates few false positives and can detect, amongst other things, errors in data downloads, rounded data, data generated by statistical procedures, and inaccurate ordering of data. These conditions would not have been easily detectable using traditional analytical procedures.

I examined this new Benford test against a data set of 23 million journal entries seeded with fraudulent entries to overstate revenues

The first time I ran the second order test I received this odd result (Figure 6):

[6] (Nigrini & Miller, 2007)

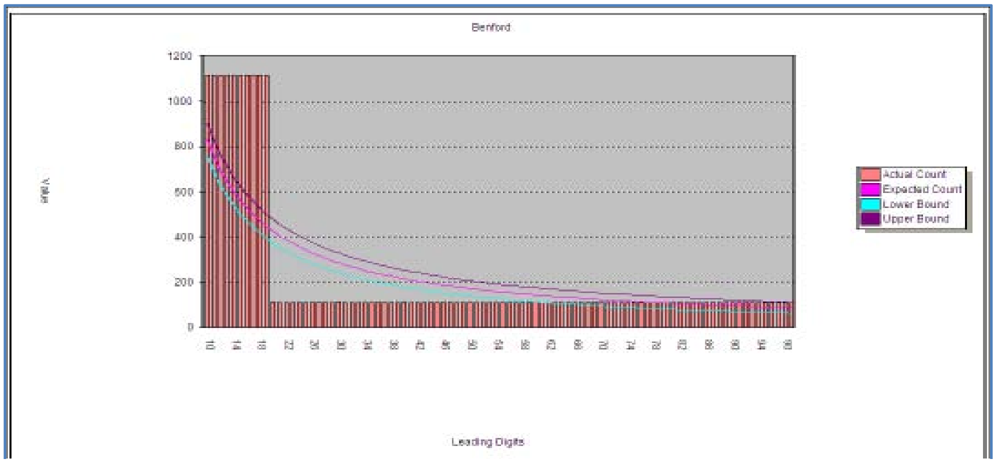


Figure 6 Benford Second Order journal entry anomaly

The first order test gave this result (Figure 7):

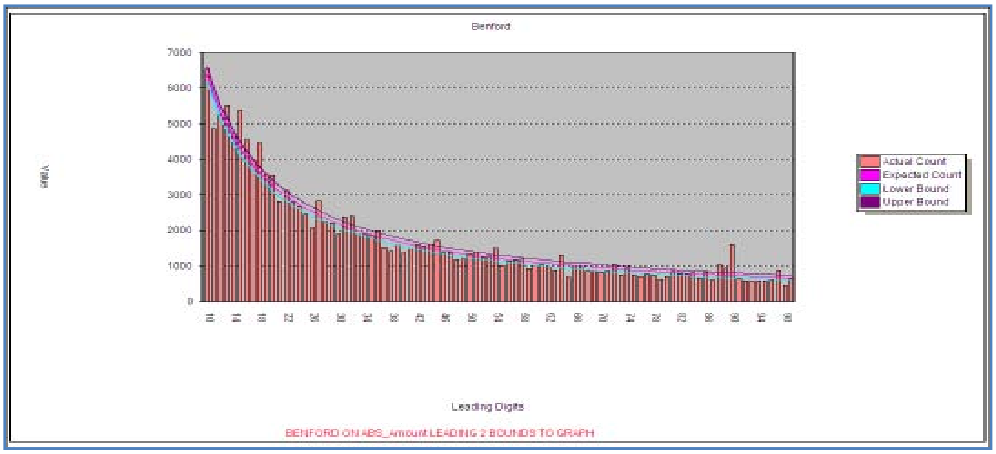


Figure 7 Benford First Order standard expected curve

Upon further investigation I found that the amounts in the posted fields of the journals were carried in the ERP system to an accuracy of three decimals but were displayed to two decimals. Clearly the test worked in that it revealed an attribute of the data that no one had suspected. After adjusting for the decimal positions the Second Order test revealed the following:

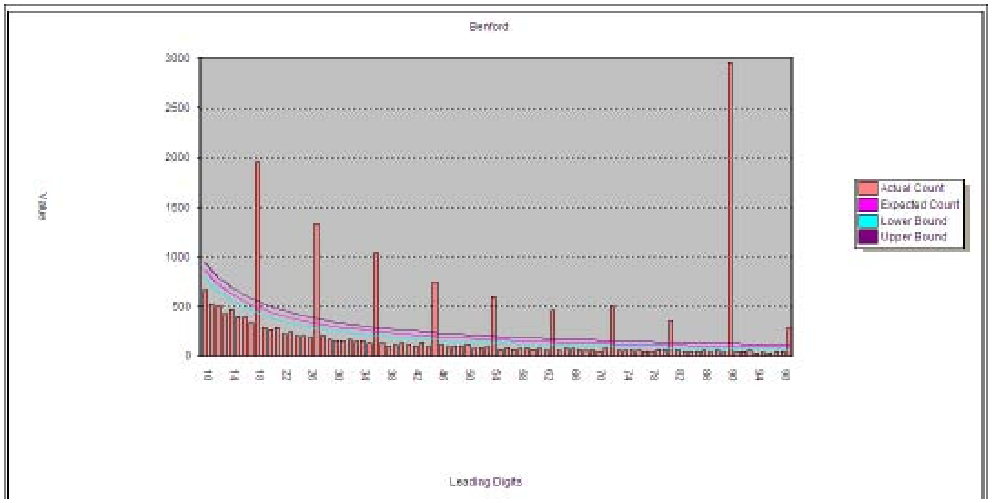
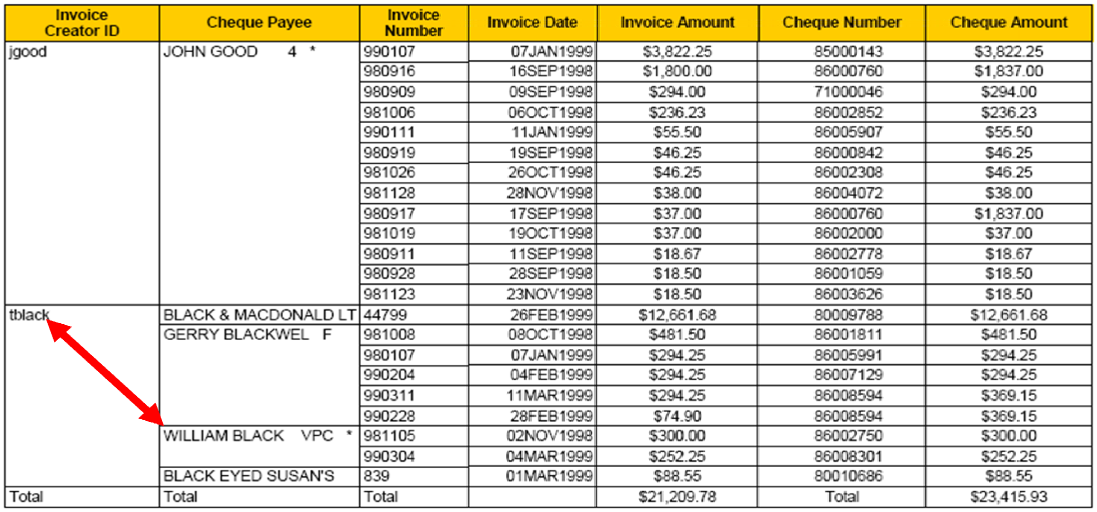


Figure 8 Benford Second Order Fraudulent journal entries

In Figure 8, above, one can clearly see the spike at the 90 level and this would prompt a further investigation by an auditor or investigator.

Fuzzy Logic

Another useful tool for an auditor or investigator is the ability to compare textual strings. I refer to this as 'fuzzy logic', which attempts to explain that the comparison of strings of data is done on a basis of an inexact match. Powerful applications, like SAS, make it possible to compare very large data sets in a short time. While many false positives might arise the system can be 'trained' to increase its precision. In this payment fraud we were able to identify payments made by a certain T Black to her husband, a VP in the company where she worked (Figure 9 below). While there were only two small payments their identification was valuable in that it provided an opportunity to identify a control deficiency that when exploited could have resulted in a substantially larger fraud over time. This illustrates the power of analytical tools to prevent fraud.



Invoice Creator ID	Cheque Payee	Invoice Number	Invoice Date	Invoice Amount	Cheque Number	Cheque Amount
jgood	JOHN GOOD 4 *	990107	07JAN1999	$3,822.25	85000143	$3,822.25
		980916	16SEP1998	$1,800.00	86000760	$1,837.00
		980909	09SEP1998	$294.00	71000046	$294.00
		981006	06OCT1998	$236.23	86002852	$236.23
		990111	11JAN1999	$55.50	86005907	$55.50
		980919	19SEP1998	$46.25	86000842	$46.25
		981026	26OCT1998	$46.25	86002308	$46.25
		981128	28NOV1998	$38.00	86004072	$38.00
		980917	17SEP1998	$37.00	86000760	$1,837.00
		981019	19OCT1998	$37.00	86002000	$37.00
		980911	11SEP1998	$18.67	86002778	$18.67
		980928	28SEP1998	$18.50	86001059	$18.50
		981123	23NOV1998	$18.50	86003626	$18.50
tblack	BLACK & MACDONALD LT	44799	26FEB1999	$12,661.68	80009788	$12,661.68
	GERRY BLACKWEL F	981008	08OCT1998	$481.50	86001811	$481.50
		980107	07JAN1999	$294.25	86005991	$294.25
		990204	04FEB1999	$294.25	86007129	$294.25
		990311	11MAR1999	$294.25	86008594	$369.15
		990228	28FEB1999	$74.90	86008594	$369.15
	WILLIAM BLACK VPC *	981105	02NOV1998	$300.00	86002750	$300.00
		990304	04MAR1999	$252.25	86008301	$252.25
	BLACK EYED SUSAN'S	839	01MAR1999	$88.55	80010686	$88.55
Total	Total	Total		$21,209.78	Total	$23,415.93

Figure 9 Example of using textual string comparison

CASE STUDY – WARRANTY CLAIMS

In this case I will illustrate the techniques discussed above and how they were applied to enable the investigator to pinpoint a fraud at a company in Canada whose main business was in selling extended warranty policies on used motor vehicles.

The client asked us to investigate claims by a car rental company for rental car invoices that were unpaid. After analysing the relevant data including the Claims Transactions File we discovered a number of **other** interesting facts.

A claim adjuster was using fictitious repair shops to process claims for cars that were under extended warranty. Using our data analysis tools we not only identified the suspicions adjuster but also alerted the client to other possible fraudsters.

We obtained the data from the client for analysis in-house. The data covered about 1 year worth of repair claims (17,640 claims). Using our analytics tools we were able to find some further anomalies such as: a car that was repaired 17 times and one that had a repair for about $11,011 dollars for an air conditioning job.

Our findings enabled the company to recover the amounts and the fraudsters were convicted and sentenced to jail.

CONCLUSION

- Fraud is now a fact of life and compliance with Sarbanes-Oxley does not guarantee no fraud will take place.
- Auditors have to consider fraud in the planning of audits.
- Solid, basic audit procedures combined with the appropriate use of technology and the dual inductive / deductive approach described above can provide an effective fraud detection process.

REFERENCES

Durtschi, C., Hillson, W., & Pacini, C. (2004). The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data. *Journal of Forensic Accounting 1524-5584 Vol. V(2004)* , 17-34.

Hodson, N. M. (2004). Detecting Fraud and Managing the Risk. *Governing the Corporation: Mapping the Loci of Power in Corporate Governance Design.* Belfast, Ireland: Queen's University.

Hodson, N. M. (2007). Presentation in Ernst & Young training conference. Toronto, Canada.

Morze, M. (1994, October 1). Publication: Business Credit. (K. C. Naff, Interviewer)

Nigrini, M. J., & Miller, S. J. (2007). *Data Diagnostics Using Second Order Tests of Benford's Law.*

PricewaterhouseCoopers. (2007). Global Economic Crime Survey.

TABLE OF FIGURES Page

CONTACT INFORMATION

Eckhardt Kriel CA (SA)

E Kriel & Associates Inc.

1148 Forest Trail Place

Oakville ON L6M 3H7

Cell: 416 451-3919

Fax: 905 847-8565

ekriel@cogeco.ca