The Problem Of False Negative Results In The Use Of Digit Analysis

Mark Linville, (E-mail: linville@ksu.edu), Kansas State University

ABSTRACT

Auditors are using the predictability of digit occurrence in recorded amounts as a tool to detect suspicious data (either erroneous or fraudulent). A key component in this type of analysis is the fact that digits naturally occur in predictable frequencies consistent with Benford's Law. This study examines the effectiveness of common digit analysis techniques in detecting the presence of suspicious data. Using data created by graduate student subjects, I find that unless the percentage of suspicious data in the population is large (> 10%) digit analysis fails to detect the presence of suspicious data. Given this propensity to produce false negative results, auditors should not rely too heavily on digit analysis as a sole or primary fraud detection tool.

INTRODUCTION

Auditors, both internal and external, are relied upon in varying degrees to detect fraud. According to professional standards, this responsibility varies depending on the magnitude and nature of the fraud and the service performed by the auditor. However, the Statement on Auditing Standards #99 has refocused the independent auditors' attention on fraud detection techniques to be used in the conduct of the independent, financial statement audit (AICPA 2002). Even if the professional standards did not require fraud consideration on a particular service, the professional would still be wise to consider it. On practical terms, if a fraud is detected primarily without auditor involvement, questions are likely to be raised about why the fraud was not detected by the auditor.

Fraudulent documents are often used in financial frauds as means of concealment (AU 316.07). Any procedure that allows auditors to reasonably detect the use of fraudulent documents is valuable. A procedure that is useful in detecting fraudulent data is likely to be useful in detecting some erroneous data as well. The term 'suspicious data' is used throughout this paper to refer to data of questionable reliability whether caused by intent (fraud) or human mistake (erroneous data). Digit analysis is a family of audit procedures that examine the pattern of digits looking for unusual patterns that could be indicative of suspicious data. Several of these digit analyses utilize Benford's Law to identify unusual digit patterns. Benford's Law suggests that the digits used to represent the size of phenomena (such as sales amounts, accounts receivable balances, expense amounts) are not equally likely to appear. Simply stated, Benford's Law says that small digits are more likely to appear in the leading digits of a number than are large digits.

The purpose of this paper is to evaluate the effectiveness of several of the common digit analysis techniques used by auditors. "Suspicious" data is seeded into "clean" data to test the effectiveness of digit analysis in detecting the presence of suspicious data. Data sets of relatively modest size are used to represent situations commonly encountered by auditors.

The results indicate that the ability of the procedures to detect suspicious data is limited. When test data represents 10% of the total sample, the methods fail to reliably detect the presence of suspicious data in these modest-sized samples. The methods appear to work somewhat better with larger samples but still lack power.

The rest of the paper is organized as follows. The next section contains a discussion of digit analysis and Benford's Law. In the third section, the methodology of the study is discussed. The results of the study are presented in the fourth section. The paper concludes with a discussion of the study's finding including limitations.

DIGIT ANALYSIS AS AN AUDIT TOOL

Several researchers have suggested the use of digit analysis as a tool for auditors to detect suspicious data (Wallace 2002, Banyard 2000, Tapp and Burg 2000, Nigrini 1999a). The actual occurrence rate or pattern of digits within the data is compared to the hypothesized occurrence rate or pattern of digits to determine if the data could contain suspicious data. Although the techniques do not identified which data points are suspicious, the techniques can alert the auditor to the possible presence of suspicious data (Lowe 2000a). In response to this heightened concern about suspicious data, the auditors can modify the nature, extent, and timing of other audit procedures.

AU § 326.11 evaluates audit procedure on two criteria: effectiveness and efficiency. The two concepts are quite distinct but often considered simultaneously. Effectiveness measures whether or not the audit procedure accomplishes its objective (in this case, does it detect suspicious data?) and efficiency measures whether or not the audit procedure provides benefits commensurate with costs incurred (in this case, is it a good use of resources?). For audit procedures, effectiveness should be paramount in order to avoid an audit failure. Effectiveness can be determined by the lack of "false negative" results provided by the methods. If an audit procedure does not reach a reasonable level of effectiveness, no amount of efficiency can justify its use. It is only when an audit procedure reaches a certain level of effectiveness that efficiency becomes a concern. Because of its primary importance, I focus on effectiveness as the evaluation criteria although efficiency is later discussed.

General Concept Of Digit Analysis

Digit analysis is assumed to work in detecting suspicious data for two reasons. First, a person creating false amounts may be unaware that he or she is creating an identifiable pattern. This may be explained in several ways. The person may subconsciously favor certain numbers. The creation of false amounts may take place over a long period of time and thus the person may not remember what falsified amounts were previously used. The person may also be biased against certain numbers in an attempt to conceal their actions. For example, a person creating false amounts often exhibits the messy-digits bias where he or she will avoid the use of amounts ending with 0s, 5s, or repeating digits. Second, the naturally occurring digits follow a pattern not known by most people. Most monetary amounts in audit situations will comply with Benford's Law (discussed later) where small digits are more likely to appear than large digits in some situations.

Regardless of the specific type of digit analysis used (Nigrini and Mittermaier (1997) review several common techniques), the same general steps are taken. First, determine the actual occurrence rate of the digit or digits to be tested. Second, determine the hypothesized occurrence rate. This occurrence rate may assume that digits occur in random fashion and thus each digit or digit pair would appear with the same frequency or the occurrence rate may follow some non-random pattern such as following Benford's Law (to be discussed in the following section). Third, compare the actual occurrence rate to the predicted occurrence rate and calculate the Z-Statistic of the difference (if any) and the related p-score. Fourth, decide whether the results suggest the presence of suspicious data. If the number of significant differences is greater than can be reasonably explained by chance, the auditor would probably conclude that suspicious data is possible. For example, if the level of significance selected is 5% (10%), the auditor could reasonably expect that approximately one of twenty (ten) observations would appear statistically significant simply by random chance.

In order to limit subjectivity in the decisions to be made on the effectiveness of the procedures, a standard decision rule is adopted. If the occurrence of significant differences on any test is greater than would be expected by simple random chance, I assume that suspicious data is indicated. Two basic types of tests are conducted. First, a test of single digits will compare the actual occurrence rate of digits to the predicted occurrence of digits in the first four digit places. In these tests, one statistically significant difference for any of the 10 digits (or 9 if the first digit place) indicate the presence of suspicious data under both the 10% and 5% levels of significance. Second, a test of the 1st

pair of digits is conducted in a similar fashion. On the tests of 1st pairs of digits, more than 5 (10) statistically significant differences out the 100 calculated differences would indicate suspicious data at the 5% (10%) level of significance. If either test indicates possible suspicious data, the population is concluded to have suspicious data. This decision rule is probably stricter than one that might be adopted in practice and completely disregards the professional judgment which might be applied by an auditor but provides consistency in this study.

Predicted Occurrence Of Digits

Benford's Law describes the occurrence of digits in naturally occurring numbers (York 2000). Probably contrary to most people's intuition, Benford's Law says that the first digit in naturally occurring numbers is more likely to be a small digit than a large digit. For example, a 1 is 6.58 times more likely than a 9 to appear in the first digit place. The distribution of digits according to Benford's Law appears in Exhibit 1.

Exhibit 1
Expected Digit Frequencies from Benford's Law

	---------- Position in Number ----------			
Digit	**1st**	**2nd**	**3rd**	**4th**
0		0.11968	0.10178	0.10018
1	0.30103	0.11389	0.10138	0.10014
2	0.17609	0.10882	0.10097	0.10010
3	0.12494	0.10433	0.10057	0.10006
4	0.09691	0.10031	0.10018	0.10002
5	0.07918	0.09668	0.09979	0.09998
6	0.06695	0.09337	0.09940	0.09994
7	0.05799	0.09035	0.09902	0.09990
8	0.05115	0.08757	0.09864	0.09986
9	0.04576	0.08500	0.09827	0.09982

The number 147 has three digits, with a 1 as the first digit, a 4 as the second digit, and a 7 as the third digit. The table shows that under Benford's Law the expected proportion of numbers with a first digit 1 is 0.30103 and the expected proportion of numbers with a third digit of 7 is 0.09902.
Source: Nigrini, Mark J., 1996. A taxpayer compliance application of Benford's Law. *The Journal of the American Taxation Association* 18 (Spring): 72-91.

Benford's Law has been found to be descriptive in many situations (Nigrini 1999b). As noted by Mark J. Nigrini in an article reprinted in Robertson (2002, page 498), based on mathematical theory and practical experience, Benford's Law applies when:

1. The data represents the sizes of similar phenomena.
2. The data has no built-in minimums or maximums, other than a minimum of zero.
3. The data does not represent assigned numbers used as descriptions or identifiers. Examples of this would be Social Security numbers, invoice numbers, telephone numbers, and bank account numbers.

The amounts on a sale invoice conform to the above requirements. The amounts represent the size of a sale transaction (requirement 1). Sales invoices have no minimums (except for zero) and no maximums (requirement 2). The amounts on the sales invoices measure size and are not artificial descriptions (requirement 3). Based on this, it is reasonable to assume that legitimate amounts on sales invoices would conform with Benford's Law and for that reason sales invoice amounts were used in data collection.

METHODOLOGY

To evaluate the effectiveness of digit analysis, I need "clean" data and "test" data. Clean data refers to the data that I created to conform to predicted frequencies and test data refers to the data created by graduate accounting students with no attempt to conform to expected frequencies. In order to evaluate the effectiveness of digit analysis, the mix of clean and test data is varied until the point at which the methods lose effectiveness is determined.

Graduate accounting students from a large, Midwestern research university created the test data. As a class exercise, three sets of students were asked at different times to help create a set of false invoice amounts. They were provided a description of the scenario including an example of 20 invoice amounts. These invoice amounts were part of a database of numbers created to conform to Benford's Law and then randomly selected to be included. The 101 graduate students participating in the exercises created 2,525 test amounts. Each time, the students were asked if anyone was aware of Benford's Law. No one claimed any knowledge of it.

Additional datasets of clean data were created. The creation of these datasets was constrained by two factors. First, this new data must conform exactly to the distribution suggested by Benford's Law at each of the first four digit places and the first two-digit pair. Second, the number of digits in the numbers in this new database must match the number of digits in the test data. The amounts ranged from a three-digit number to a seven-digit number.

To test the effectiveness of digit analysis, the mix of test and clean data is varied. When less than 100% of the test data is needed, a random selection process is used to determine the data to be included in the sample. This process is repeated for each new trial.

As mentioned earlier, digit analysis has several types of procedures that can be used to determine the validity of data of which I select the two most basic. First, a test of the frequency of occurrence of single digits in each of the first four digit places is performed. In this test, the occurrence of each digit at each digit place is tested against the hypothesized occurrence rate (for example, if Benford's Law applies, the digit "1" should appear in the first digit place 30.103 % of the time, in the second digit place 11.389 % of the time). I chose to perform this test to the fourth digit place resulting in 39 tests (the digit "0" cannot appear in the first digit place) in each trial. The distribution of digits in the first four columns as determined by Benford's Law is not random. The distribution of digits in the fifth digit place is approximately random as can be seen by a simple extrapolation of the first four columns onto what would be the fifth column in Exhibit 1. Second, the frequency of occurrence of the first two digits is tested. The occurrence rate of the first pair of digits can be compared to the hypothesized occurrence rate. The frequency of the digit-pair occurrence is calculated by determining the joint probability of the particular digits appearing in the first and second digit places.

The effectiveness of the procedures is tested in two ways to determine if the procedures produce false negative results. First, the procedures are evaluated in their ability to detect the existence of suspicious data through a series of tests with each successive test having a smaller proportion of test data comprising the sample being tested. This is continued until the procedures fail to detect suspicious data, the "failure" point. Once this "failure" point is identified, random samples of test data are drawn and mixed with clean data at approximately the "failure" proportion. This is done to determine that the "failure" point is due to the particular data used or if it represents a more general failure point.

RESULTS

Tests Of Digit Analysis' Ability To Detect Suspicious Data

The first test on the ability of digit analysis to detect suspicious data uses a sample consisting of 100% suspicious data. Of course, for digit analysis to have any effectiveness, it must be able to detect suspicious data is such a situation. The results of the test are reported in Table 1 for the sample of 2,525 observations.

Table 1
Results of Digit Analysis with 100% Test Data

Analysis of Single Digits							
	1st Digit				2nd Digit	3rd Digit	4th Digit
Digit	**Actual**	**Predicted**	***Z*-stat**	***p*-value**	***p*-value**	***p*-value**	***p*-value**
0	NA	NA	NA	NA	0.7948	**0.0488**	**0.0026**
1	668	760	-3.9958	**0.0001**	**0.0078**	**0.0015**	**0.0014**
2	381	445	-3.3243	**0.0012**	**0.0001**	**0.0000**	**0.0002**
3	256	315	-3.5795	**0.0005**	**0.0250**	**0.0990**	0.3576
4	244	245	-0.0469	0.9680	0.6100	0.1868	**0.0784**
5	235	200	2.5847	**0.0098**	0.1556	**0.0052**	**0.0220**
6	212	169	3.4199	**0.0007**	**0.0142**	0.8414	0.2262
7	208	146	5.2429	**0.0000**	0.9282	0.8886	0.7872
8	179	129	4.5028	**0.0000**	0.4354	0.2262	0.8886
9	142	116	2.5195	**0.0000**	0.6892	0.1556	0.8494

Actual = number of times digit is observed in the 1st digit place in the population.
Predicted = number of times digit should be observed in the 1st digit place in the population.
Z-stat = $\frac{\text{actual} - \text{predicted}}{[\text{number} \times \text{probability} \times (1 - \text{probability})]^{1/2}}$
p-value = probability of observing the difference between actual count and predicted count due to random chance.

Table 1 shows the analysis of single digits with additional information provided on the analysis of the 1st digit. Similar analysis is performed for digit places 2 through 4 but only the *p*-values are reported. In the analysis of the first digit place, eight digits have a frequency of occurrence significantly different than predicted at the 5% level of significance. In the analysis of the second through fourth digit place, 14 (13) of the 30 digits have a frequency of occurrence significantly different than predicted at the 10% (5%) level of significance. Using the decision rule described earlier, the data appears to contain suspicious data.

Table 2 shows a similar single-digit analysis of the data from multiple samples in which the proportion of test and clean data is varied. The first six columns of row one of Table 2 summarize the results reported on Table 1. A 5% level of statistical significance is used on this table. Each sample adds more clean data to the test data in order to determine at what point digit analysis loses it ability to detect the suspicious data, the "failure" point. In addition, a test of the first pair of digits is performed on each sample.

Table 2
Tests for Bounds of Effectiveness
5% Level of Significance

%	N	1st digit	2nd digit	3rd digit	4th digit	1st pair	Suspicious Data Detected?
100%	2,525	**8**	**4**	**4**	**4**	**20**	yes
50%	5,050	**6**	**1**	**3**	**3**	**14**	yes
33%	7,575	**5**	**1**	**1**	**1**	**8**	yes
25%	10,100	**3**	**1**	**1**	0	3	yes
20%	12,625	**2**	0	0	0	3	yes
16.67%	15,150	**1**	0	0	0	3	yes
14.29%	17,675	**1**	0	0	0	1	yes
12.50%	20,200	0	0	0	0	0	no
11.11%	22,725	0	0	0	0	0	no
10%	25,250	0	0	0	0	0	no

% = percentage of suspicious data contained in population.
N = total population size.
n^{th} digit = number of digits in n^{th} digit place significantly different than predicted.
1st pair = number of pairs of digits in the first two digit places which are significantly different than predicted.
Suspicious Data Detected = Using the predetermined decision rule, was the presence of the suspicious data detected in the population.
Numbers in bold represent unexpectedly high number of statistically significant results.

As shown in Table 2, at a 5% level of significance, the test of single digits detects suspicious data until the test data represented 12.50% of the population. The tests involving the first digit place seem to be more discriminating than the tests involving the second through fourth digit place. The test involving the fourth digit place could not detect suspicious data when test data represented 25% of the population, while the tests involving the second and third digit place could not detect suspicious data when test data represented 20% of the population. As discussed later, this increased discriminating ability is probably due to the uniqueness of the distribution specified by Benford's Law.

As shown in Table 2, the ability of the test of the first pair of digits to detect suspicious data is somewhat limited. The tests could not detect suspicious data when test data represents 25% of the population.

Table 3 reports the results of the same set of tests except this time using the 10% level of statistical significance. The test of the first digit place is effective until the proportion of test data reached 10% of the population. The tests of the second and fourth digits could detect the suspicious data until it reached the test data reached 16.67% level of the population. The test of the third digit place is effective until the test data reaches the 14.29% level of the population. The test of the 1st digit pair is unable to detect suspicious data when the test data represented 25% of the population.

Table 3
Tests for Bounds of Effectiveness
10% Level of Significance

%	N	1st digit	2nd digit	3rd digit	4th digit	1st pair	Suspicious Data Detected?
100%	2,525	**8**	**4**	**5**	**5**	**22**	yes
50%	5,050	**8**	**3**	**3**	**3**	**21**	yes
33%	7,575	**6**	**1**	**2**	**3**	**11**	yes
25%	10,100	**6**	**1**	**1**	**1**	8	yes
20%	12,625	**3**	**1**	**1**	**1**	5	yes
16.67%	15,150	**2**	0	**1**	0	5	yes
14.29%	17,675	**2**	0	0	0	3	yes
12.50%	20,200	**1**	0	0	0	3	yes
11.11%	22,725	**1**	0	0	0	1	yes
10%	25,250	0	0	0	0	0	no

% = percentage of suspicious data contained in population.
N = total population size.
n^{th} digit = number of digits in n^{th} digit place significantly different than predicted.
1st pair = number of pairs of digits in the first two digit places which are significantly different than predicted.
Suspicious Data Detected = Using the predetermined decision rule, was the presence of the suspicious data detected in the population.
Numbers in bold represent unexpectedly high number of statistically significant results.

In order to determine if the results observed are simply an artifact of the specific data used, I conduct tests on ten additional samples. The samples are prepared by randomly selecting 1,000 items from the 2,525 amounts created by the graduate students. This data is combined with 7,000 clean amounts to create a series of trials with the test data representing 12.50% of the population. The 12.50% level is selected arbitrarily. However, it does represent the point at which the tests seem to be unable to detect suspicious data while using the 5% level of statistical significance.

As reported in Table 4, digit analysis cannot detect suspicious data in any of the ten trials. The results show nothing that would suggest suspicious data to all but the most skeptical of auditors.

Table 4
Additional Trials
10% level of significance

Trial	N	1st digit	2nd digit	3rd digit	4th digit	1st pair	Suspicious Data Detected?
1	8,000	0	0	0	0	0	no
2	8,000	0	0	0	0	0	no
3	8,000	0	0	0	0	1	no
4	8,000	0	0	0	0	1	no
5	8,000	0	0	0	0	1	no
6	8,000	0	0	0	0	0	no
7	8,000	0	0	0	0	0	no
8	8,000	0	0	0	0	0	no
9	8,000	0	0	0	0	1	no
10	8,000	0	0	0	0	0	no

N = total population size. In each trial, 1,000 observations were randomly selected from the test data and combined with 7,000 clean observations.
n^{th} digit = number of digits in n^{th} digit place significantly different than predicted.
1^{st} pair = number of pairs of digits in the first two digit places which are significantly different than predicted.
Suspicious Data Detected = Using the predetermined decision rule, was the presence of the suspicious data detected in the population.
Numbers in bold represent unexpectedly high number of statistically significant results.

DISCUSSION

The primary conclusion of this paper is that digit analysis, in all the tested forms, has little effectiveness in detecting relatively large percentage of suspicious data in modest-size samples. Using a 5% (10%) level of statistical significance, single-digit tests could not detect suspicious data when the test data comprised 12.50% (10%) of the population. Test of the 1^{st} pairs of digits performed even worse. In 10 additional trials, digit analysis could not detect suspicious data when 12.50% of the population is test data. In 1,390 separate tests performed in these trials, only 4 differences between actual and predicted occurrences achieved statistical significance at the 10% level and no significant differences are not when the 5% level of statistical significance is used. Failure to detect suspicious data at a proportion this high seems to suggest that digit analysis is a weak test for the presence of suspicious data. Even in the most corrupt or inept organizations, it is hard to imagine that one of eight sales invoices is fraudulent or in error.

The inability of the methods to conclusively detect the presence of suspicious data when test data comprises a large portion of the population has serious ramifications to auditors who are relying on digit analysis to detect suspicious data. Although a financial statement auditor only provides reasonable assurance of no material misstatements in the financial statements due to fraud or error, an auditor who fails to detect fraud, when specific fraud techniques are applied, is vulnerable to charges of negligence. Due to this high failure rate, the auditor who uses digit analysis should use the techniques in conjunction with other procedures. Nigrini and Mittemaier (1997) and Busta and Weinburg (1998) make similar suggestions about the necessity of additional information to supplement the initial findings of digit analysis when used as an analytical procedure.

Given the inability of the techniques to detect relatively-large portions of suspicious data in the population, it seems somewhat pointless to test for the techniques propensity to produce false positives. Since the power of the tests to detect legitimately suspicious data is weak, it is not likely to produce false positive results. While not tested in this paper, the possibility of the techniques to yield false positives does have serious ramifications to the auditor. Digit analysis is designed to detect the presence of suspicious data, not to pinpoint which items are suspicious. Given the new emphasis on fraud detection as detailed in the Statement on Auditing Standards #99, the auditor cannot ignore a fraud indicator without strong evidence to negate the indicator (AICPA 2002). The auditor responding to a false positive indication of suspicious data is chasing a ghost and will have to accumulate volumes

of evidence to substantiate that suspicious data does not exist. In other words, the auditor is put in the difficult situation of having to prove a negative and as a result the efficiency of the audit suffers.

The use of digit analysis can be justified despite its apparent lack of effectiveness because of its efficiency. An auditor with access to a client's accounting records through generalized auditing software can perform these procedures inexpensively (Albrecht 2002, page 148). Even if lacking in effectiveness, adding some forms of digit analysis adds little costs to the audit. Additionally, as pointed by Lowe (2000b), the analysis of divergences from Benford's Law almost always provides useful insights. These insights can reveal errors and processing inefficiencies as well as revealing fraud.

Among the different general types of digit analysis, the test for the first digits is the most effective in detecting suspicious data. The first digit place is where the distribution of Benford's Law differs the most from a random distribution. As the distribution of Benford's Law becomes more like a random distribution, its ability to detect suspicious data weakens. This may explain why the test using the 1st pair of digits is less effective than the test for first digits. By using the joint distribution, the uniqueness of the distribution of first digit place under Benford's Law is diluted by the more randomly-distributed second digit place.

The use of digit analysis necessitates the use of the proper assumptions to establish the predicted frequencies of digit occurrence and care must be taken in establishing the predicted frequencies. Several factors can skew the frequencies and if the auditor does not know of these the possibility of a false positive increases. For example, consider a company that uses a pricing scheme with all prices ending in 99 cents and operates in a jurisdiction with no sales tax. Although all combinations of the last two digits are possible, .01 as the last two digits can be obtained on a sales invoice only if the number of items purchased ends with the digits 99 (such as 99 items, 199 items, etc.). These transactions are possible but somewhat unlikely. If the auditor assumes that all combinations of the last two digits are equally possible, the digit analysis on the last two digits is likely to lead to misleading results.

Limitations To The Study

This study is subject to limitations. Proponents of digit analysis admit that the techniques are most appropriate in large populations (Wallace 2000). Part of the purpose of this study was to determine its applicability in a sample of a size more commonly encountered by an auditor. However, the relatively small sample sizes may have doomed the techniques to failure in this study. In addition, the process of collecting data is likely different than the situation facing an employee committing fraud. Subjects were asked to provide 25 fraudulent amounts at one time rather than over an extended period of time. Persons performing a fraud over an extended period of time are unlikely to remember what amounts were previously used and fall into habits that can lead to their detection. Subjects in this study can easily review previously-created fraudulent amounts and possibly avoid obvious patterns. Finally, the subjects had no aids, such as a computer or previous knowledge of Benford's Law, to assist them in the creation of fraudulent numbers.

ACKNOWLEDGEMENTS

I would like to thank the participants at the Kansas State University workshop series, the Southwest Business Symposium, and the American Accounting Association – Midwest Region for their comments on this paper.

REFERENCES

1. Albrecht, S. W. (2002). *Fraud Examination* (1st ed.). Cincinnati, OH: Thomson Southwestern.
2. American Institute of Certified Public Accountants (AICPA). (2002). *Statement on Auditing Standards, Consideration of Fraud in a Financial Statement Audit*, New York, NY: AICPA.
3. Banyard, P. (2000). A new aid for fraud detection. *Credit Management* (March): 32-33.

4. Busta, B. and Weinberg, R. (1998). Using Benford's law and neural networks as a review procedure. *Managerial Auditing Journal* 13 (6): 356-366.
5. Lowe, R. (2000a). Benford's law and fraud detection. *Chartered Accountants Journal of New Zealand* 79 (10): 32-36.
6. Lowe, R. (2000b). When Benford's law is broken. *Chartered Accountants Journal of New Zealand* 79 (11): 24-27.
7. Nigrini, M. J. (1996). A taxpayer compliance application of Benford's Law. *The Journal of the American Taxation Association* 18 (Spring): 72-91.
8. Nigrini, M. J. and Mittermaier, L. J. (1997). The use of Benford's law as an aid in analytical procedures. *Auditing: A Journal of Practice and Theory* 16 (2): 52-67.
9. Nigrini, M. J. (1999a). Adding value with digital analysis. *Internal Auditor* 56 (1): 21-23.
10. Nigrini, M. J. (1999b). I've got your number. *Journal of Accountancy* 187 (5): 79-83.
11. Robertson, J. C. (2002). *Fraud Examination for Managers and Auditors* (2002 ed.). Austin, TX: Viesca Books.
12. Tapp, D. J. and Burg, D. B. (2000). Using technology to detect fraud. *Pennsylvania CPA Journal* 71 (4): 20-23.
13. Wallace, W. A. (2002). Assessing the quality of data used for benchmarking and decision making. *Journal of Government Financial Management* 51(3): 16-22.
14. York, D. (2000). Benford's law. *Accountancy* 126 (July): 126.

NOTES

NOTES