icameka
THE 2ND INTERNATIONAL CONFERENCE
ACCOUNTING, MANAGEMENT, ECONOMICS, UNISKA

E-ISSN 3089-1566

Proceeding Accounting, Management, Economics Uniska **Volume 2, 2025, pp 282-290**

"The Role of Research in Economics, Management, Accounting to Realizing Sustainable Development"

The Patterns of the Numbers used in Occupational Fraud Schemes

Bella Paradita[1], Eko Prasetyo [2*] ,Ita Yoeli Astari [3]
[1]Universitas Kahuripan Kediri
***Email:** bellaparadita@kahuripan.ac.id

ABSTRACT

Purpose - This study aims to determine the numbers used in financial statement fraud, corruption, and asset misappropriation schemes, thus enabling the design of an effective proactive analytics-based fraud detection test.Design/Methodology/Approach - The data sources used in this study were court records related to fraud prosecutions, investigative reports, and research papers related to fraud cases.Findings - Fraudulent numbers are most often round numbers, have strong period-to-period growth, fall just above or below internal control thresholds or other targets, are deviations from Benford's Law, are deliberate duplicates of authentic transactions, are outliers due to their excessive size, and are excessively rounded up or down. Limitations/Research Implications - The sample may not be representative of the population of detected and undetected frauds. Further research is needed to detect corruption/bribery schemes.Practical Implications - The results of this study are important for auditors and forensic accountants conducting proactive fraud detection tests. The discussion emphasizes that the analysis should include refinement and retesting, and then use clustering and filtering to address false positives. Originality/Value - This research provides an original, in-depth coverage of the patterns found in fraudulent numbers. The discussion section addresses implementation issues and considerations for future research.

Keyword:scheme, fraud, investigative

INTRODUCTION

The objective of this study is to classify the numbers used in recent fraud schemes in such a way that these classes can be used to design effective proactive analytics-based fraud detection tests. This classification is important because organizations currently face a host of internal, external, regulatory, and reputational fraud-related risks. Anti-fraud activities have become a core business issue as the scale and the impact of fraud has grown in our digitally enabled world. Fortunately, innovative technologies such as monitoring, data Occupational fraud schemes can be broadly classified as either being asset misappropriation, corruption, or financial statement fraud (ACFE, 2018). Asset misappropriation occurs when a fraudster (internal or external) uses deception to misuse, misapply, or divert an organization's resources or assets for a personal gain. Corruption, also known as bribery, occurs when one person gives or offers something valuable to another person in a position of trust so as to influence his/her judgement or conduct. Financial statement fraud occurs when a fraudster presents manipulated financial reports (or misrepresented financial data) so as to mislead investors, auditors, and analysts about an entity's true financial condition.

The financial services sector leads the field in using advanced technologies and techniques, such as analytics and alerts issued by a continuous monitoring application, to fight fraud. With respect to these tools, some companies invest in emerging technologies that they do not use optimally, while others are late adopters and find themselves falling behind the curve. With respect to forensic analytics, organizations are deriving value from activities such as continuous monitoring, periodic analysis, transaction testing, proactive detection, anomaly detection, unstructured data reviews and pattern recognition (PWC, 2018).

The literature lacks a case-based guide for external auditors and forensic accountants to determine which analytics tests might be effective in a proactive fraud detection exercise. There is not much guidance for those professionals who want to assess whether their set of analytics tests is suited to the fraud detection task at hand. Forensic accounting textbooks typically refer to running proactive fraud detection tests as the "detection of analytical anomalies." Their discussions range from providing a laundry list of tests with very few case studies to support these tests, to a short list of tests with only a handful of case studies supporting the suggestions. Tests described as "deviations from specifications" or "no pattern when you would expect one" offer no specifics and might need data that is difficult to obtain or that is not captured in a payment processing system. It is unfortunately not in the self-interest of a forensic accountant who has detected a fraud using analytics to publicly share their specific tests at a public conference or in a magazine article. The paper describes seven categories of fraudulent number patterns: round numbers, rising numbers, threshold numbers, non-Benford numbers, repeated numbers, outlier numbers, and rounded numbers. Each of the categories is described in greater detail below, including, where available, real-world case studies illustrating the patterns and a short discussion section evaluating some relevant practical and technical issues. The concluding comments highlight, amongst other things, the fact that the number patterns relate better to some fraud schemes than to others, as well as the importance of a high degree of skepticism during the manual review of the notable items.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

2. Fraudulent numbers

This section describes the seven patterns observed in the fraudulent numbers used by fraudsters in their fraud schemes. Table I shows that the fraudulent number patterns are relevant to either one, two or three of the occupational fraud schemes described in the introduction.The numeric and behavioral consistencies, derived from court documents and various reports, provide support for forensic accountants running related analytics tests to identify high-risk situations in their own data or in their client's data. The discussion sections examine some of the practical issues relevant to identifying high-risk situations Occupationalfraud schemes 603 (e.g. transactions, vendors, audit clients, financial reports or employees) based on their number patterns.

2.1 Round numbers

Round numbers get press coverage when they relate to targets or benchmarks. In 2017, newspaper articles reported that the stock prices of Amazon and Alphabet (the parent company of Google) had crossed the $1,000 mark (Wall Street Journal, 2017). The fact that the Dow Jones had crossed the 25,000 mark was a recent Wall Street Journal (2018a) frontpage story. In our everyday lives, round numbers such as 10-year anniversaries or 100-degree days act as key reference points.

Round numbers are seen in many types of frauds such as, financial statement fraud, bribery and asset misappropriation schemes. With respect to financial statement frauds, America Online (AOL) used round numbers in its scheme to artificially inflate its online advertising revenue (SEC v Kelly, Rindner, Ripp, and Wovsaniker, 2008). AOL padded its advertising revenue by: paying inflated prices to vendors;

overpaying for business acquisitions; and accepting less than the fair value in the settlement of business disputes, all with neutralizing side agreements for the purchase of online advertising. For example, AOL agreed to forego a 15 per cent discount on equipment purchases from SunMicrosystems. It reported the $37,500,000 foregone discount as advertising revenue and took delivery of equipment as payment in lieu of cash for the advertising. AOL also agreed to overpay a software supplier by $20,000,000 on the understanding that the supplier would then purchase online advertising for $20,000,000. It also agreed to overpay a hardware supplier and a data transmission company by $12,000,000 and $15,000,000 respectively.

AOL also converted the proceeds of two business disputes into online advertising of $12,500,000 and $23,800,000. As part of an account reconciliation exercise, AOL deliberately overpaid WorldCom by $34,200,000 with a side agreement that it purchase online advertising for that amount. In SEC v. Years and Doody (2016), the controller capitalized labor of $104,000 and overhead of $265,000 to Work in Process ("WIP") at the end of the third quarter of 2012. Thiswas repeated at the end of the fourth quarter by capitalizing labor of $124,000 and overhead of $346,000. When the external auditors made inquiries about the fourth quarter journal entries, the controller informed the COO and sent the auditors a spreadsheet that supported

2 Rising numbers

Rising numbers refer to transaction totals that increase at an abnormally high rate overtime. The reason for the rapidly rising numbers (or totals) is because, loosely speaking, fraudsters do not know when to stop. They keep pushing the limits. "These people have convincedthemselvesthattheywon't get caught" (Wells, 2012, p. 54). An example of an asset misappropriation scheme that used rising numbers was the scheme of Charlene Corley, and her twin sister Darlene Wooten, which was featured on the television series American Greed a (Season 4, Episode 35) and on Evil Twins (Season 2, Episode 2). Corley worked at the South Carolina Budget and Control Board before starting C&D Distributors. The original products sold were highway and street signs, but the business later changed to an appliance delivery service. As a sideline, C&D Distributors also sold hardware components, plumbing fixtures, and small electrical items to the Department of Defense through an online bidding system. The Defense Finance and Accounting Service ("DFAS") office that made the payments to Corley's firm did not audit or control the shipping charges paid. From 1997 to 2006, Corley's firm submitted fraudulent claims for shipping charges that were linked to valid invoices for hardware, plumbing, and electrical items. The firm submitted about 500 fraudulent invoices for shipping charges totaling $71.6m, of which the DFAS paid 112 invoices totaling $20.58m. The fraud scheme ended when the firm submitted the following two false claims for shipping charges on the same:

METHODS

The data sources for the classification scheme include the court
records of fraud prosecutions, investigative reports and research papers related to fraud cases. Findings – Fraudulent numbers are most often amounts that are round, have a strong peri

RESULTS

Not all transactions that are just below a threshold are fraudulent or notable. The challenge is to identify which transactions or items have been strategically

control-related activity. For example, past experience with vendor invoices shows that computer-related vendors and furniture vendors price their products at amounts such as $499 or $999, a phenomenon known as just-below pricing. These amounts are just below the thresholds of $500 and $1,000. It is also possible that a seller might accept a sales price of $2,500 (a typical maximum amount for purchasing cards) from a buyer that can more conveniently pay using his or her purchasing card. In an income tax setting, a US taxpayer might claim a deduction of less than $500 to avoid having to complete and submit Form 8283 with her tax return if the value of the noncash donation is marginally above $500. Similarly, a USA taxpayer might claim a deduction of less than $5,000 to avoid having to submit a qualified appraisal with noncash donations worth just slightly more than $5,000. A first-two digit Benford analysis (discussed in more detail below) might help to detect threshold-avoiding behavior in environments where a forensic account is unsure of what thresholds might be influencing people's behavior. In this case the analysis would focus on spikes at first-two digits that are just below neat multiples of 10 (10, 20, 30, ..., 90) or multiples of 5 (10, 15, 20, ..., 95). For example, a spike at 24 for travel and expense reimbursements might indicate that employees are excessively claiming expenses of $24 because a voucher is required for expenses of $25 and above. A spike at 24 for purchasing card transactions might indicate that employees are excessively spending (and perhaps splitting purchases) when the amounts are above $2,500 since most cards have a $2,500 spending limit for a single transaction.

External auditors need to be aware of materiality-related thresholds. Auditing Standard 2810 of the Public Company Accounting Oversight Board (PCAOB), Evaluating Audit Results (PCAOB, 2015a) states that an intentional misstatement could be material for qualitative reasons, even if it is a relatively small (i.e. quantitatively immaterial) amount. Examples include misstatements that: distort the true trend; change a loss into a profit; distort segment information; affect compliance with loan covenants, contractual agreements or regulatory

provisions; have the effect of meeting incentive compensation hurdles; and are a misclassification between recurring or infrequent items.

In these scenarios, a small, seemingly immaterial misstatement could have the effect of making a threshold that otherwise would have been missed. The issue here is that the auditor cannot simply search for transactions below a certain numeric amount.

DISCUSSION

The final step in running a "rising numbers" test on (say) vendors is to rank the vendors, from those showing the biggest increase over time to those showing the smallest increase over time. The same would apply to ranking employees by overtime hours, MAJ 34,5 608 or the members of a loyalty program by points earned. The best option is to use data over anextended period of time, since that is more indicative of a trend than data covering just two years or perhaps just two half-years. To reduce the number of false positives, forensic accountants should understand that alarge percentage increase might not be indicative of a fraud if the prior and current amounts are small. For example, a $100 annual total that increases to $600 in the next year is a large percentage increase, but it is an increase from a small base. Cases such as these can be excluded from the sample of notable items. Also, a percentage increase cannot be calculated for a series of amounts that starts at zero (e.g. a percentage increase cannot be calculated for $0-$600-$1,000 because it would require a division by zero). Finally, forensic accountantswould need to formulate a logical heuristic to determine whether a pattern of $100-$500-$1,000 shows a larger rising numbers trend than does a pattern of $100-$600-$1,000.This test could generate an audit sample that is impractical to manually review for anorganization with many vendors, employees, or loyalty program members. The test can berefined to identify large percentage increases together with large increases in absolute values. The large sample issue can be further addressed by grouping vendors into risk categories and by focusing on the high risk categories. For example, an airline might consider jet fuel vendors to be low risk in an environment where oil prices are increasing. Incontrast, vendors that supply services to a head office that are charged to a "Maintenance Building" account and not allocated to any specific operating unit could be identified as highrisk.

2.3 Threshold numbers

Threshold numbers are numbers that are a level, point, or numeric value at which something is true. When thresholds are related to internal controls, they are a level, point, or numeric value at which additional checks or procedures will take place. A perceived control threshold is an amount that a fraudster, a corporate outsider, believes to be a control threshold. Other descriptions of the same concept are hurdles or targets (such as blood pressure readings) which have possible significant consequences, giving people a tendency or a disposition to act in a certain way.An early example of using thresholds to identify financial statement misconduct was by

Carslaw (1988) who used Benford's Law ("Benford") to show that corporate earnings tend to

be rounded-up above key numbers or cognitive reference points (N * 10k numbers where N and k are integers). For evidence of this phenomenon, he looked at the proportion of second digit zeroes in reported net income amounts. For example, if a true net income amount of $1,985m was rounded up to $2,004m, and if this type of rounding-up was done by several companies, then a table of net incomes would have an excess of second digit 0s ($2,004) and a shortage of second digit 9s ($1,985). Carslaw's study has generated a stream of research,and Geyer and Drechsler (2014) summarize twelve studies that used Benford to detect rounding-up behavior around cognitive reference points.Benford was also used to detect an asset misappropriation scheme in which an electricutility company was investigating the theft of electricity (Nigrini, 2012). The first step in theoriginal analysis was to identify customers with large decreases in billing amounts, which resulted from stealing previously purchased electricity. This test produced an impractically large sample of notable items; a second test analyzed the kilowatt-hour (kWh) amountscredited to customer accounts. Selected results are shown in Figure 1.The first-two digits' graph in Panel A of Figure 1 shows that the actual proportion for the 99s is about twice as large as the Benford proportion (Nigrini, 2017). The next step was to select all the first-two digits 99 credits and then to sort the credits from largest to smallest. The top values are presented in Panel B, which shows that the kWh credits were numbers just below the perceived thresholds of 106 and 105. The full list of notable items showed about 200 amounts just below 100,000 kilowatt hours. The follow-on investigation found that collections personnel were giving customers large kWh credits in exchange for kickbacks. Lynn Scheufler was the controller and chief financial officer ("CFO") of three highend nightclubs at the Foxwoods Casino in Connecticut. She was responsible for generating sales reports, monthly statements, accounts receivable and accounts payable, payroll transactions, preparing company checks, and the financial accounting. She was also responsible for replenishing the automated-teller machines ("ATMs") with cash. At the end of each day, the nightclub managers put their daily cash sales in a bag in a drop safe. The managers prepared a deposit slip showing the number of bills for beach denomination and the total dollars in the bag. To replenish the ATMs, Scheufler used cash from the nightly deposit bags. Instead of removing only enough cash to refill the ATMs and then preparing a new deposit slip for the new total, Scheufler apparently removed excess cash from the nightly deposit bags. From mid-2010 to mid-2012, a total of $2,534,009 was removed from the nightly deposit bags over and above what was placed in the ATMs. Scheufler denied taking the money, but was still charged with the fraud due to her andher husband's attempt to avoid detection through structuring (USA v. Scheufler and Galligan, 2012). It is a felony to structure transactions for the purpose of evading the reporting requirements for cash deposits of $10,000 or more. Scheufler's cash deposits for2011 are shown in Table III.

Table III shows that most of the cash deposits were for round multiples of $100. During the second half of 2011, many $9,900 deposits were made, which is just below the $10,000 reporting requirement. A bank employee told the investigator that Scheufler's husband would bring deposits consisting of two strapped bundles of $5,000 each, and that before

CONCLUSION

fraud schemes could be used as the basis for rules-based proactive fraud detection tests. Asshown in Table I, most of the fraudulent number patterns are related to financial statement fraud, and slightly fewer are related to asset misappropriation fraud schemes. Identifying these number patterns in corporate data will produce large samples that will usually be too extensive to review given the auditor or forensic accountant's time constraints. These tests could be rerun in an iterative fashion, and grouping and filtering could also be used to reduce the number of notable items (AICPA, 2017). Filters could be used to delete small items. The dollar amounts in asset misappropriation schemes are unlikely to be small because these are not worth the risk of being caught. The final analysis will include a manual review of the notable transactions. This manual review should be carefully executed because this will ultimately determine whether a fraud is detected. The importance of the review is illustrated in the $48.3m fraud scheme of Harriette Walters described in Jacoby et al. (2011). Her fraud is also described in an investigative report, and extracts from that report note the following:Between 2002 and 2006, the auditors selected a total of 190 real property tax refunds for testing with specific, limited procedures, which did not include reviewing the underlying documentation supporting the refunds. The samples included seven of Walters' fraudulent refunds and one credit associated with a fraudulent refund. We found no evidence that the auditors identified these refunds as improper (Gray and Evans, 2008 , p. 5). Some District auditors did identify internal control weaknesses and large revenue variances relevant to real property tax refunds. Had there been follow-up on the identified control weaknesses or deeper investigation into the revenue variances, Walters' scheme might have been discovered earlier (Gray and Evans, 2008, p. 79). The investigative report stated that the audit samples included some fraudulent refunds that were not detected by the auditors. It also noted that her fraud might have been detected by athorough review of the control weaknesses and the revenue variances. Ineffective auditing of the sample counteracts the effectiveness of identifying a valid sample of notable items. Future research could report the results of running proactive fraud detection tests using the number patterns discussed in this study. Additional research could review number patterns found in fraud schemes in other countries and attempt to explain any observed differences. Future research could also address the apparent difficulty.

REFERENCES

Baker, C. and Hayes, R. (2004), "Reflecting form over substance: the case of Enron corp", Critical
Perspectives on Accounting, Vol. 15 Nos 6/7, pp. 767-785.
Beresford, D., Katzenbach, N. and Rogers, C. (2003), Report of Investigation by the Special Investigative
Committee of the Board of Directors of WorldCom, Inc., WorldCom Inc., Clinton, MS.
Carslaw, C. (1988),"Anomalies in income numbers: evidence of goal oriented behavior", The Accounting
Review, Vol. 63 No. 2, pp. 321-327.
Daigle, R., Louwers, T. and Morris, J. (2013), "HealthSouth, Inc.: an instructional case examining auditors' legal liability, teaching notes", Issues in Accounting Education, Vol. 28 No. 4, pp. 10-24.
Das, S. and Zhang, H. (2003), "Rounding-up in reported EPS, behavioral thresholds, and earnings management", Journal of Accounting and Economics, Vol. 35 No. 1, pp. 31-50.
Debreceny, R. and Gray, G. (2010), "Data mining journal entries for fraud detection: an exploratory study", International Journal of Accounting Information Systems, Vol. 11 No. 3, pp. 157-181.Geyer, D. and Drechsler, C. (2014), "Detecting cosmetic debt management using Benford's law", Journal of Applied Business Research (Jabr), Vol. 30 No. 5, pp. 1485-1492. Gray, V. and Evans, J. (2008), Report of Investigation, Office of Tax and Revenue Investigation Special Committee, Washington, DC, available at: www.dcwatch.com/govern/otr081215.pdf (accessed 23 September 2018).
Jacoby, P., Lorigo, S. and McCallum, B. (2011), "Fraudulent tax refunds: the notorious career of Harriette
Walters", Current Issues in Auditing, Vol. 5 No. 1, pp. A23-A38.
HealthSouth (2004), "Report of the special audit review committee of the board of directors of HealthSouth
corporation", available at: www.sec.gov/Archives/edgar/data/785161/000095017204001357/ex99-1hsc.txt (accessed 23 September 2018). Nigrini, M. (2012), Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection, John Wiley, Hoboken, NJ.Nigrini, M. (2016), "The implications of the similarity between fraud numbers and the numbers in
financial accounting textbooks and test banks", Journal of Forensic Accounting Research, Vol. 1
No. 1, pp. A1-A26.
Nigrini, M. (2017), "Audit sampling using Benford's law: a review of the literature with some new
perspectives", Journal of Emerging Technologies in Accounting, Vol. 14 No. 2, pp. 29-46.
Nigrini, M. (2018), "Round numbers: a fingerprint of fraud", The Journal of Accountancy, Vol. 225 No. 4,
pp. 36-42.

Nigrini, M. and Mueller, N. (2014), "Lessons from an $8 million fraud", Journal of Accountancy, Vol. 218
No. 2, pp. 32-37.
Pedneault, S. (2010), Fraud 101: Techniques and Strategies for Understanding Fraud, John Wiley,
Hoboken, NJ.
PwC (2018), "Global economic crime survey", available at: www.pwc.com/gx/en/services/advisory/
forensics/economic-crime-survey.html#cta-1 (accessed 23 September 2018).
Public Company Accounting Oversight Board (PCAOB) (2015a), Evaluating Audit Results: Auditing
Standard 2810, PCAOB, Washington, DC.
Public Company Accounting Oversight Board (PCAOB) (2015b), Audit Sampling: Auditing Standard 2315, PCAOB, Washington, DC. Securities and Exchange Board of India ((2014), "Order in the matter of Satyam computer services ltd",available at: www.wsj.com/public/resources/documents/Satyam.pdf (accessed 23 September
2018). SEC v Kelly, Rindner, Ripp, and Wovsaniker (2008), Case 1:08-cv-04612-CM-GWG, US District Court, Southern District of New York, NY. SEC v. Years and Doody (2016), Administrative proceeding 3-17278, available at: www.sec.gov/litigation/admin/2016/34-78017.pdf (accessed 23 September 2018).Occupationalfraud schemes
621 Smith, W. (2013), "Lessons of the HealthSouth fraud: an insider's view", Issues inAccounting Education,