A fraud investigation plan for a false accounting and theft case

Mark Eshwar Lokanan

Faculty of Management, Royal Roads University, Victoria, Canada

Abstract

Purpose – The purpose of this paper is to formulate and propose a fraud investigation plan that forensic accountants can use to investigate financial frauds. In particular, the paper sets out the structure and rationale of the fraud investigation plan that both forensic accountants and fraud examiners can use in their investigation of false accounting and theft charges.

Design/methodology/approach – The paper uses the material facts from the Polly Peck International fraud as a prototype case upon which to build an investigation plan and detail potential areas of investigation to establish evidence for a criminal trial.

Findings – The findings revealed that the case can be used to provide insights on evidence gathering techniques and test particular models of fraud detection. The concealment and conversion evidence gathering techniques provide fodder on how to gather and triangulate both direct and circumstantial evidence that can be used to avoid mistrials in courts.

Practical implications – The case is of interest to practitioners and forensic and fraud examination students who would like to build on their existing knowledge and obtain insights into the steps to follow to conduct an investigation and gather evidence to build a case. The paper makes specific recommendations to enhance the effectiveness and efficiency of investigations.

Originality/value – The paper is among one of the few to propose a fraud investigation plan designed to investigate cases involving false accounting and theft charges. More importantly, the paper uses a real case to illustrate how to examine documentation/data and how such documentation will be analysed in a trial.

Keywords Fraud, Benford's law, Neural networks, Algorithm, Decision trees, Investigation plan

Paper type Case study

1. Introduction and background

Polly Peck International (PPI) was a large UK-based company that was quoted on the London Stock Exchange (LSE). PPI started with an astute investment by Asil Nadir ("Nadir") of a small textile company called Polly Peck. In the late 1970s, under the management of Nadir, PPI used Nadir's stock market status to raise cash and set up a "Northern Cyprus fruit-packing subsidiary, Sunzest and Unipac, a cardboard box factory, via a share issue" (The Telegraph, 2012, para. 8). During the next four years, PPI expanded into consumer electronics, hotel franchises and fruit and vegetable packaging in Europe and expanded internationally. The expansion and rise in demand for PPI's product led to a rise in its stock price at the LSE. In 1983, PPI share price reached a high of £35 but crashed after rumours that the Turkish Government was about to withdraw vital tax concessions. By the early 1990s, PPI's share price recovered and sent its shares skyrocketing. The company made stratospheric profits and was worth £2bn making it a financial times stock exchange 100 player (Casciani, 2012, p. 11). In the summer of 1990, there were persistent rumours concerning opaque accounting methods and manipulation of PPI's share price, which had reached an intensity that could no longer be ignored by regulatory authorities, including the Serious Fraud Office (SFO) (The Telegraph, 2012, para. 16).

On 19 September 1990, the SFO raided one of Nadir's management companies. The next day, PPI's share price plummeted and the company completely collapsed in 1991. The SFO initially began investigating PPI for insider trading, what they found instead was a complex scheme wherein Nadir had stolen millions of pounds that belonged to PPI's shareholders. It is alleged that Nadir was moving money offshore without requiring the signatures of other directors. Nadir was able to steal the money from PPI by authorising or instructing the transfer of the stolen fund from the company's London bank accounts and hiding them through complex transactions in offshore accounts. Nadir had the power to do this because PPI was too dependent on him. He was both the chairman and chief executive of the company when it collapsed.

In the trial, the prosecution alleged that from August 1987 onwards, Nadir, assisted by his close associates, "used more than 50 transfers to steal approximately £150m from PPI" (Casciani, 2012, para. 15). Prosecutors claimed that in total, £34m in cash had been withdrawn from London bank accounts and filtered through accounts in Switzerland, the Channel Islands, PPI subsidiaries and a bank in northern Cyprus controlled by Nadir. During the trial, the court heard "that Nadir used some of the cash to protect PPI's stock-market valuation by buying its own shares. The largest single chunk of the missing £150m went to margin lenders, a sophisticated form of borrowing to buy shares, tied to the value of the stock" (Casciani, 2012, para.18). His autocratic management style allowed him to use the stolen money to purchase shares and shares options in PPI both in his name and in the name of others (including family members) who may have been nominees. Ultimately, however, a chunk of the stolen money was used to acquire and fund various business ventures, properties and trusts controlled by Nadir, his family and close associates.

The purpose of this paper is to formulate and propose a fraud investigation plan that forensic accountants can use to investigate cases like the PPI. In particular, the paper will set out the structure and rationale of the fraud investigation plan. More specifically, the focus will be on the accounting manipulation of PPI's books, the theft charges levelled against Nadir and the tracing of the proceeds of the ill-gotten gains. To gain insight into these issues, the structure of the report will proceed according to the following format. First, I will present an investigative plan detailing the potential areas to gather evidence. Second, I will conduct an analysis of the methods to obtain evidence. Third, I will present a formal proposal of the recommendations to take the investigation forward.

2. The investigation plan

2.1 Developing the investigation plan

The first step in the investigation process begins with predication. Predication is the fact or event that triggers the investigation (ACFE, 2014). In PPI's case, predication arose from innuendos, financial irregularities and unorthodox transactions, which raised suspicion that Nadir was transferring funds from his London accounts to foreign subsidiaries. The task is to start with an assessment of the predication that Nadir is hiding assets but to be very wary that investigative resources will quickly become overloaded if every tip or rumour is investigated to the fullest possible extent. Cognisant of resource limitations, the investigation plan starts out with the null hypothesis that Nadir is innocent and there is no fraud. This is the process in a court of law. The accused is innocent until proven guilty. The investigation will attempt to reject the null hypothesis. At this juncture, the investigation team is encouraged to not be derelict in their duty to follow up valid leads.

As such, to develop the context of the case, the following questions are proposed:

Q1. Who is hiding the asset?

Q2. What motivated the individual to hide the asset?

Q3. How did the individual hide the asset?

Developing the context will assist in scope out the investigation in the early stages of the planning process and helps with efficiency, time-wasting and monetary resources (ACFE, 2014). Part of the scoping phase should involve the following consideration in developing the investigation plan:

- pay attention to see if the proceeds of the fraud are commingled with other assets (not linked to the fraud) that Nadir owned;
- be aware that the stolen funds may flow through various channels;
- be aware that Nadir may avoid holding assets or accounts in his own name to conceal his role in the fraud;
- because Nadir may avoid holding asset or accounts in his own name, investigation effort should be geared to other associates who may be involved (e.g. relatives, business associates, straw men, corporate vehicles such as trusts, LLPs, foundations, etc.); and
- the investigation team must assess whether it is feasible to seize assets discovered in the course of gathering information.

At the planning stage, it is beneficial to conduct a cost-benefit analysis to estimate the total monetary value being stolen and to decide whether the loss is sufficient enough to continue with the investigation. Here it is useful to use the Bayesian approach and Beneish M-Scores model for fraud detection to filter out unnecessary information. As the investigation proceeds, working theories are either strengthened or discarded because of the lack of relevance to the investigation. In applying the Bayesian approach, the investigators will have prior probabilities, which they will then update to posterior possibilities (Albrecht *et al.*, 2001):

$$P(B/\text{A}) = \frac{P(B/A)}{P(A)}(P/B)$$

Where:
  B = Fraud; and
  A = Evidence.

Therefore:

- $P(B/A)$ is the *prior* of what is believed about the fraud (B) before encountering new evidence (A);
- the *posterior* probability is what is believed about the fraud (B) after having encountered new evidence (A); and
- the *quotient* of the likelihood of fraud divided by the *marginal probability* of the new evidence forms part of the informativeness of the new information for the belief about fraud (B).

Therefore, the updated Bayesian approach formula is:

$$P(Fraud|Evidence) = P\big[(Evidence|Fraud)/(Evidence)P(Fraud)\big]$$

To further filter the information from the initial predication, the investigation team can also use the Beneish M-Score to test for earnings manipulation. The Beneish (1997) M-Score is a mathematical model that is used to analyse whether a company has manipulated its financial statements. The M-Score uses five-variable and eight-variable financial ratios to test for earnings manipulation in companies' financial reports. The M-Score formulae are:
Five-variable model:

$$M = -6.065 + 0.823\,DSRI + 0.906\,GMI + 0.593\,AQI + 0.717\,SGI + 0.107\,DEPI$$

Eight-variable model:

$$M = -4.84 + 0.92\,DSRI + 0.528\,GMI + 0.404\,AQI + 0.892\,SGI$$
$$+ \ 0.115\,DEPI - 0.172\,SGAI + 4.679\,TATA - 0.327\,LVGI$$

Where:
DSRI = Days' sales in receivable index;
GMI = Gross margin index;
AQI = Asset quality index;
SGI = Sales growth index;
DEPI = Depreciation index;
SGAI = Sales and general and administrative expenses index;
LVGI = Leverage index; and
TATA = Total accruals to total assets.

Once calculated, the results from the five and eight variables are combined to form two separate M-Scores. M-Score of less than -1.78 suggests that the company did not manipulate its earnings, while an M-Score that is higher than -1.78 indicates that the company has manipulated its earnings (Beneish *et al.*, 2013).

2.2 Collecting information
Following the results of the forensic models, the next stage of the investigation is to focus its resources to collect information that matters about the stolen funds. With regard to Nadir, audit documents, business cards, personal records, internet and interviews with associates and acquaintances will be conducted to gather the following information on Nadir:

- date of birth, identities of close relatives, friends and business associates; and
- Nadir's national insurance number, last known address and the names of his close relatives.

The purpose of this basic information is to gather intelligence to trace the stolen funds. Relevant information can be obtained from the London banks and bankers that Nadir dealt with in the UK special investigative techniques such as physical surveillance and witness interviews can be used to keep abreast of Nadir's actions and whereabouts. The investigation team may want to obtain authority from the court for civil orders for Nadir to produce relevant financial information, to conduct interviews in PPI's London offices and subsidiaries, and review records on-site. The investigation team may also want to obtain information by conducting private records search, records of relevant real estates and other financial accounting information. It is hoped that this search will lead to potential leads that include information regarding foreign accounts, assets, persons and entities.

3. Create subject profile

3.1 Business profile

The investigation team should also build a business profile of PPI. A business profile will assist the team to understand PPI and the several industries it was in and will show any unusual occurrences arising from its operations. The business profile is used to prove the movement of stolen funds by Nadir from the point of payment or transfer from the accounts of PPI or any other entities of the PPI's group. The first step is for the investigation team to determine how PPI is organised and structured. This information will provide leads to information relating to the incorporation of the various entities that make up the PPI group. Next, the investigation team should identify the key personnel associated with the business. This personnel includes spouse, board of directors, the individuals directly involved in the suspected transactions (i.e. bankers, clerks, secretaries and key present and former employees), accountants and consultants. The investigation team should next identify the money flow patterns of the suspected transaction (i.e. where the money came from and where it is heading), locate all of PPI's bank accounts and authorised signatures and determine the Company's financial conditions to uncover possible motive of Nadir's actions. All of Kakos's business records (financial statements and tax returns) should also be reviewed to show its overall financial conditions.

3.2 Analyse the information

The investigation team should then proceed to review and analyse the information collected. The investigation team should critically evaluate the data and look for potential leads that can feed the investigation. In this particular case, potential leads may include accounts, assets, entities, properties and names of family members, friends and associates. To identify the stolen funds, the investigation should focus on incorporation, partnership agreements with PPI's foreign entities and bank statements, legal filings and any other documents that may reveal ownership of entities and assets and how they were used. When reviewing these documents, the investigator should look for cheque signing authority. There is evidence to suggest that Nadir had sole cheque signing authority on various accounts. An effort should also be made to analyse electronic data such as e-mails accounts, phone registers and any other database that can give valuable leads to indicate that Nadir may have transferred assets. The financial records collected should then be analysed to trace stolen funds. The analysis should look for unexplained variance in income and expense in PPI's accounts and Nadir's lifestyle.

3.3 Conduct interviews

At this stage, the investigation team should begin conducting interviews with parties who may have valuable information on the stolen funds and where Nadir is concealing his assets. It is expected that the information obtained during the interview will corroborate information obtained from the documentary evidence regarding the stolen funds and explore new leads.

3.4 Trace stolen assets

After all the documents have been collected, the investigation team should begin reviewing the financials and begin tracing the stolen funds. In PPI's case, tracing involves the movement of funds in and out of the London accounts, and in particular, a search for funds stolen by Nadir to find the accounts and destinations into which the money is being channelled. The investigation team may also want to identify key individuals, organisations (i.e. banks) and the connection between them and the financial flow of the missing funds.

The information in Nadir and PPI's financial profile can be compared with the information of any suspicious transaction (e.g. dates, account holders, destinations and banks) to individuals or groups and reconciled to identify gaps in the data.

4. Models and methods to gather and provide evidence

The models used to gather evidence are concealment and conversion. Concealment techniques focus on how the fraudster disguises his actions to steal funds from PPI without detection (Albrecht *et al.*, 2012). Concealment methods will endeavour to provide evidence of the stolen funds, while conversion methods will provide circumstantial evidence in support of the evidence gathered from the concealment technique. Based on the accounts of the case, it is likely that Nadir may have used his authority to manipulate the books and audit trail to obscure the fraud. As a result, this aspect of the investigation is mostly focussed on the techniques to gather evidence of Nadir's criminogenic actions. The conversion aspect of the evidence gathering process focusses on how the fraudster benefited from the proceeds of crime (Albrecht *et al.*, 2012). Based on the evidence from previous behavioural fraud research (Morales *et al.*, 2014; Lokanan, 2015), Nadir may have to use the proceeds to improve his current lifestyle or live a luxurious lifestyle. An examination of Nadir's spending habits can be triangulated with other fraud methods to potentially identify the missing funds.

4.1 Concealment method

4.1.1 Building a financial profile. When trying to locate stolen funds, the first step is to build a financial profile of the main suspect (ACFE, 2014; Comer, 2003; Wells, 2014). The financial profile shows the outflow of cash and other liabilities (expenses) attributed to the suspect, as well as the inflow of cash and other revenue (income) coming of the suspect over a period of time. In other words, the financial profile shows the suspect's financial condition. There are two approaches to establish Nadir's financial profile: direct and indirect approach.

4.1.2 Direct approach. The direct approach to tracing stolen funds uses direct evidence to investigate a subject's financial profile and lifestyle (ACFE, 2014). This approach uses the subjects' accounting and financial information to identify accounts, assets and expenditures and trace the source of funds for each. In Nadir's case, the investigation team should focus attention on the following sources to build his financial profile: documents from the banks and other financial intermediaries with whom he deals. The investigation team may also want to look at tax records (both foreign and local), accounting reports and financial statements of all entities, bank accounts, credit reports and court records. It is hoped that by thoroughly reviewing these sources, the investigation team will be in a good position to identify funds coming into and out of various accounts and any increase or decrease in account balances. Given the nature of Kakos' fraud, it is highly likely that direct evidence of the stolen funds may not be available or the investigators will be denied access to Nadir and PPI's books and records. In such a scenario, the investigation team must turn to the indirect approach.

4.1.3 Indirect approach (net worth method). The indirect approach uses circumstantial evidence to analyse the subject's financial position (Block, 1969; Healy and Palepu, 2003; Simser, 2008). The investigation team can use several sources to identify whether Nadir was living beyond his means and build a financial profile. Interviews can be conducted with Nadir and his associates where possible. Close scrutiny should also be on Nadir's lifestyle, his assets (i.e. his residence, vehicles, etc.), business filings and records (e.g. through the companies' register and information held by the stock exchange), real estate records, charitable contributions, travel records (frequent flyers club), bankruptcy records,

accounting work papers, tax returns and financial statements. The investigation team can also look into previous government intelligence reports of Nadir and audit reports of PPI.

To prepare Nadir's financial profile, the investigation will follow the following steps for the relevant period. First, identify all assets held by Nadir. Second, identify all his liabilities (or debt) arising from written promises to pay at a set date. Third, identify all sources of revenue during the relevant period being investigated. Fourth, identify all of Nadir's expenses incurred. Fifth, once the investigation team has identified Nadir's assets, liabilities, income and expenses, and assigned those values, they should have enough data to calculate Nadir's net worth. While Nadir's net worth is circumstantial proof, it can be corroborated with testimony of co-conspirators (i.e. his bankers, associates, etc.) as circumstantial evidence that he stole from PPI. It is expected that the network statement will give investigators a complete financial profile of Nadir and PPI's operations (Comisky, 1981; Manning, 2005; Albrecht *et al.*, 2012).

To triangulate the evidence from the indirect approach, the investigators should use the asset method and the expenditures to verify Nadir and PPI's finances (Comisky, 1981). This approach is based on the theory that the funds available to a person during a period of time are either applied to increase his net worth (i.e. assets less liabilities) or spent on personal living expenses (e.g. food, rent and vehicle operating expenses) (Block, 1969; Comisky, 1981; Comer, 2003; Wells, 2013). Accordingly, the total of the increase in a person's net worth over any given period, plus the total of his or her living expenses, will equal the total income received. The difference between this figure and the funds available from known sources is what is of interest to the investigator. To put this into context, as there are suspicions regarding Nadir's increased net worth, the asset method should be used to examine whether he has invested illegal funds to accumulate wealth and acquire assets (Adkisson and Riser, 2004; Albrecht *et al.*, 2012; Lokanan, 2014). From all accounts, Nadir was still jetting around Europe, Cyprus and Turkey to save his empire. As such, the expenditure method should be used to see how this affects his net worth. The increase in Nadir's net worth and expenditure should be compared with the available legitimate funds. The investigation team can infer that unaccounted funds may come from illegitimate sources.

4.1.4 Building a business profile. The investigation team should also build a business profile of PPI (ACFE, 2014, pp. 37-41). A business profile will assist the team to understand PPI and the several industries with which it dealt. Unusual occurrences from operations will become transparent. The business profile is used to prove the movement of stolen funds by Nadir from the point of transfer from the accounts of PPI or any other entities of the PPI group. To provide leads relating to the incorporation of the various entities that made up the group, the first step is for the investigation team to determine how PPI was organised and structured. Next, the investigation team should identify the key personnel associated with PPI. This personnel includes Nadir's spouse, relatives, board of directors, individuals who may have been directly involved in the suspected transactions (i.e. bankers, clerks, secretaries and present and former employees), accountants and consultants. Efforts should be made to identify the money flow patterns of the suspected transaction (i.e. where the money came from and where it was heading), locate all of PPI's bank accounts and authorised signatures and determine the company's financial condition to uncover possible motives for Nadir's actions. All of PPI's business records (financial statements and tax returns) should also be reviewed to show its overall financial condition.

4.1.5 Bank deposit method. The investigation team should also look at the bank deposit method for potential evidence of the case. Given that Nadir is alleged to have stolen about £34m in cash, particular emphasis should be placed on the total deposit method to look for round sum amounts (£100,000, £150,000, £200,000, etc.) going out of the account. That is,

the investigators should look to detect the accounts and destinations into which the stolen funds were being channelled.

4.1.6 Asset tracing. Asset tracking is vital to Nadir's transportation of the funds. The funds could have been converted to travellers' cheques and deposited into bank accounts in Cyprus (and Turkey). The investigation team should trace assets to see if the funds were used to buy assets in these countries.

4.1.7 Direct tracing. Assuming that the books and records of PPI are in reasonable good condition and are accessible, direct tracing of funds can be carried out to help the investigation team to identify the nature, description, ownership and location of assets funded by the stolen money for possible seizure. Direct tracing can also be done to identify the individuals and/or entities with knowledge of the criminal funds and the assets that were acquired with the funds and identify the areas on which to focus during discovery and other examinations. The investigation team should look for the existence of an audit trail to establish a chain of evidence. This will allow them to follow the transaction from the London accounts through to the banks and the respective accounts into which the funds may have been deposited (Albrecht *et al.*, 2001). Once these are identified, the investigation team should look at who owns the banks and conduct interviews with these individuals. When following the audit trail, the investigators are encouraged to look in either direction:

- follow specific transactions from their origin forward to the point of interest; and
- follow the stream of evidence from summary reports back to its sources (Albrecht *et al.*, 2012).

Tracing forward shows that the transactions have been reported completely and accurately while tracing backward from summary to origin ensures that the summary figures are based on actual transactions.

4.1.8 Indirect tracing. When the banks and accounts are not known or the suspect and witnesses are unwilling to supply information, a financial profile of the suspect can be built by the indirect method of tracing to demonstrate that the target had funds that did not come from known, legitimate sources (Eads, 1991). This approach is based on the net worth analysis, which is similar to the indirect method used to build a financial profile and provide evidence for the investigation. As it pertains to the present case, Nadir can use his contacts to transfer assets to family members or other related third parties, which will still allow him to maintain control. He may protect the assets by transferring them and opening children or family trust accounts or prepay a significant portion of his mortgages on properties (homes), insurance or credit cards, etc.

5. Conversion method
5.1 Behavioural profile
The behavioural profile complements the financial profile and provides possible motives for Nadir's actions (Dorminey *et al.*, 2010; Lokanan, 2014; Wells, 2014). Here it is useful to incorporate the fraud triangle as a methodology used to gather evidence of fraud. The fraud triangle posits that for fraud to occur, three elements must be present – the pressure, opportunity and motivation to commit the criminogenic act. Although the fraud triangle has been criticised to reflect that financial pressure is deemed an incomplete descriptor of fraud (Dorminey *et al.*, 2010) – given that opportunity does not address collusive behaviour (Morales *et al.*, 2014; Lokanan, 2015) and rationalisation is not an observable trait (Murphy and Dacin, 2011) – it can be applied in this case because Nadir's behaviour from all accounts stems from his own behaviour rather than the action of the collective.

The key here is to use the fraud triangle to gather information about Nadir's motivation, the opportunities available to steal funds and his lifestyle from interviews and other documentary sources (ACFE, 2014, p. 36). Information collated from the behaviour profile can attest to Nadir's personal characteristics and lifestyle habits. Data should be collected on his personal characteristics (amount of cash he carries, designer clothing, expensive watches and jewellery), lodging (expensive hotels and vacation homes), transportation (exotic vehicles and luxury cars) and his leisure activities (cruises, expensive vacations and planes) (ACFE, 2014, p. 36). Evidence of a luxurious lifestyle should be corroborated with cash withdrawals from his disclosed bank account(s). Where this is not the case, then Nadir may have other undisclosed account(s) that need to be investigated (ACFE, 2014, p. 37).

6. DATA mining techniques

6.1 Benford's law
The investigation team should use various proven data mining techniques to assemble and analyse the data. One of the tests that can be used to collate and examine evidence is Benford's law (Nigrini, 2011). Benford's law test examines the occurrence of first digit distribution and the occurrence of two digits distributions in fraud cases. Given that Nadir was stealing funds from PPI's London accounts, Benford's law can be used to detect anomalies (whether by theft or random acts) in the data gathered. As can be seen in Figure 1 below, for naturally occurring data, one should expect the first digit of integer:
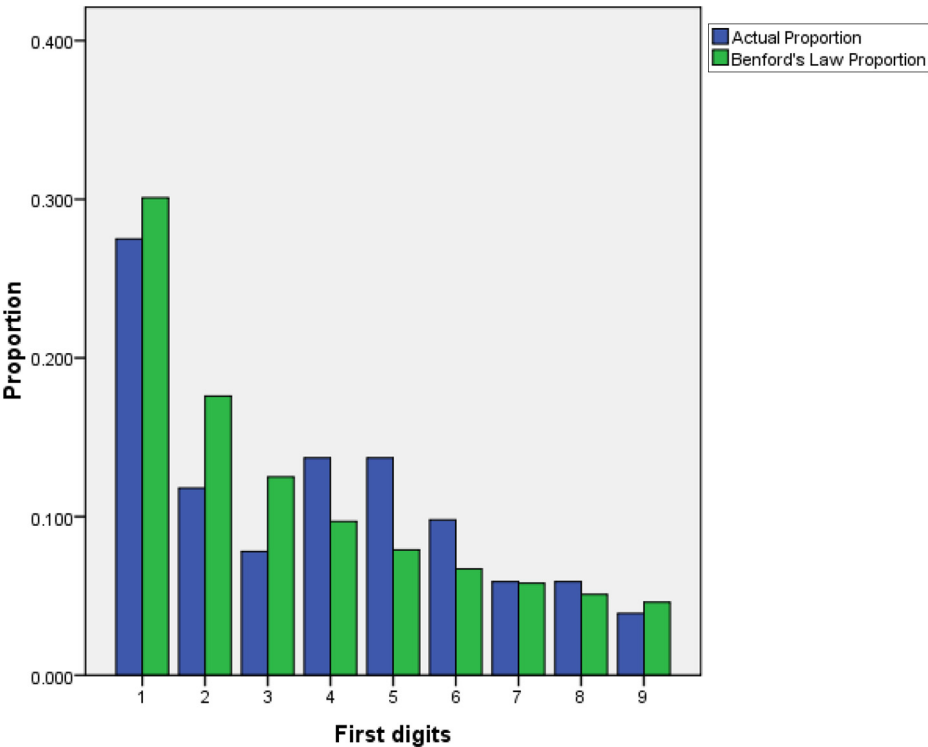

Figure 1.
Bar graph showing Benford proportion against the actual proportion

- to occur about 30 per cent of the time and integer; and
- to occur about 18 per cent of the time.

The same logic applies when two digits are used with a slight variation in the percentage of time they occur. Using Benford's distribution of the occurrence of the first digit, one would expect to find the frequency of the digit "2" (of, for example, 297.60) occurring more frequently than the predicted frequency about 18 per cent of the time. Using the distribution of the first two digits, one would expect to find the digits "29" as in the first two digits (of, for example, 297.60) occurring more often than the predicted frequency of about 20 per cent of the time. This is because, for each set of stolen funds, there will be a series of numbers that are credited, which will show the actual frequency of the digits "2" and "29" occurring much more frequently than the expected frequency of the digits "2" and "29".

6.2 Decision tree
Another useful data mining techniques for fraud investigation is decision trees. A decision tree "is a tree structure wherein each node represents a test on an attribute and each branch represents an outcome of the test" (Kirkos *et al.*, 2007, p. 998). In this way, the tree divides observations from the evidence into mutually exclusive subgroups for further analysis (Kirkos, Spathis and Manolopoulos, 2007, p. 998). Decision Trees can be used to describe and filter the data to provide useful input for decision making. Figure 2 below shows a decision tree where Nadir may have sprinkled stolen funds of less than $100,000 to banks and funds of more than $100,000 to his family members. Algorithms can then be used to validate the transactions of the funds from one account to another.

6.3 Artificial neural networks
Artificial neural networks are a technique used in fraud detection mainly in the context of supervised classifications (Calderon and Cheh, 2002). Neural networks are a data mining technique that "consists of a number of neurons, i.e. interconnected processing units" (Kirkos *et al.*, 2007, p. 999). Associated with each connection is a numerical value called "weight", which combines with the signals from other connecting neurons to calculate a combined input signal (Kirkos *et al.*, 2007, p. 999). When the combined input signals are
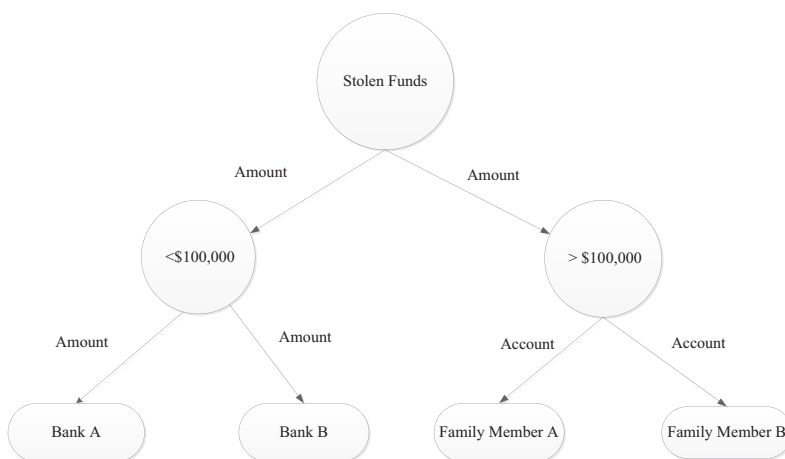
Figure 2.
Decision tree showing movements of alleged stolen funds

greater than the threshold, then the neurons fire off. As it applies to fraud detection, when a neuron network detects significantly more transactions than normal, the input value is transformed by the transfer function and fires off, which raises red flags that fraud might be taking place (Han and Camber, 2000). Thus, the input signal for neuron b is:

$$ub = Rwib * xi$$

wherexi is the input signal from neuron i and wib is the weight of the connection between neuron i and neuron b.

In Figure 3 below, the network receives an input vector (indicator) of fraud and connects it to the hidden layer (where weights are assigned, i.e. W_1, W_2, W_3 and W_4). The combined weights are then connected and processed by an output layer and fire off a fraud alert neuron (i.e. output).

6.4 Goodness-of-fit-test
The chi-square (χ^2) goodness-of-fit-test can also be used to detect Nadir's fraudulent activities. In this case, all the data assembled on the stolen funds will be tabulated using Excel or any other statistical software (Minitab, SPSS, etc.) to evaluate how close the observed values are with what is usually expected. As with Benford's law, the information will be grouped into bar graphs so that the observed values and the expected values can be eyeballed and analysed for meaningful inferences. Any discrepancies will be red flagged for further investigation. The expectation is that the actual distribution will not approximate the expected amount. More specifically, the actual distribution of the funds stolen will not be what is normally expected from the hypothesised distribution of the data collated. That is, the null hypothesis is that the dollar value of the funds recovered followed the expected distribution and is rejected for an alternative hypothesis, which says that the dollar value of the stolen funds does not follow a specified distribution.

7. Recommendation for the investigation
To determine the factual basis of the allegations of fraud by Nadir, the investigation team should first use the data collected and build a personal and financial profile of Nadir and PPI. In developing the profile, the team should be aware that the stolen funds may have been commingled with other assets (not linked to the fraud) in Cyprus and Turkey. The stolen funds may change form as they flow through various channels orchestrated by Nadir (ACFE, 2014, p. 25). Nadir may also try to avoid transferring the accounts into funds in his
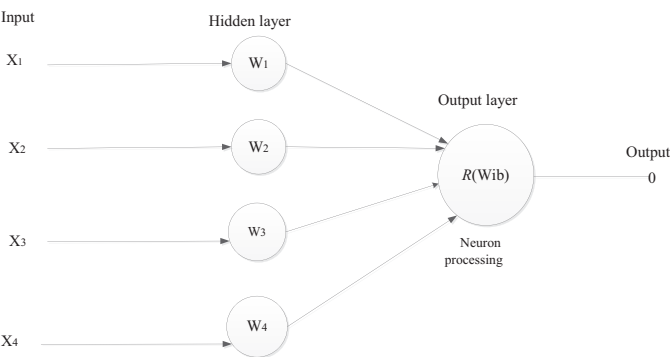

Figure 3.
Neural network algorithm

name; as such, the investigation team should also examine the accounts of family members, friends and associates who may be involved in the scheme.

The investigation team should use both the direct and indirect methods to build Nadir's financial profile. The direct method approach to Nadir's financial standing and profile should be triangulated with the direct method of asset tracking. It is assumed that as a publicly traded corporation, the books and records (or at least some of them) of Nadir and PPI are in reasonably good order and, as such, direct tracing of transactions and funds through the business or through a person's hands, maybe possible (Kovalerchuk *et al.*, 2007; Lokanan, 2014). Corporate fraud takes a long time to plan and execute (Albrecht *et al.*, 2001; Adkisson and Riser, 2004). As such, the books and records of Nadir and PPI may be falsified or at best inaccurate. Accordingly, the information from such records should be corroborated with other information.

One way to corroborate direct evidence is with indirect or circumstantial proof. The emphasis should be on analysing the relationship between Nadir's receipts and his subsequent disposition of funds (ACFE, 2014, p. 32). The investigation team should also triangulate the indirect method of building Nadir's net worth with the indirect method of asset tracking. These various indirect methods are used to detect whether Nadir was able to accumulate funds that did not come from legitimate sources. Together, the indirect method to build Nadir's financial profile and the indirect approach to tracing his asset can give investigators a good idea of his net worth. The indirect approach should also be triangulated with Nadir's behavioural profile. This will assist investigators to analyse whether the stolen funds were either spend on lavish lifestyle purchases or invested. The total of the funds applied to lifestyle purchases or investment must be equal to the funds available from all legitimate sources. The excess funds may represent illegal income and should be investigated.

To conclude, the investigation team should triangulate the data to corroborate evidence to be used in court. There is a high possibility that some of the direct evidence may not be accurate, and consequently, may not hold up during cross-examination. The direct and indirect approaches can work together to prove the existence of the principal fact, with a combination of inference and without inferences or presumptions regarding Nadir's actions. Evidence presented in this manner is deemed admissible and relevant and may form a link in a chain of evidence that may lead to a successful prosecution and reject the null hypothesis.

References

ACFE (2014), *Making Crime Pay: How to Locate Hidden Assets*, ACFE, Austin, TX.

Adkisson, J. and Riser, C. (2004), *Asset Protection: Strategies for Protecting Your Wealth*, McGraw-Hill, New York, NY.

Albrecht, C., Albrecht, S. and Dunn, G. (2001), "Conducting a pro-active fraud audit: a case study", *Journal of Forensic Accounting*, Vol. 2 No. 2, pp. 203-218.

Albrecht, W., Albrecht, C., Albrecht, C. and Zimbelman, M. (2012), *Fraud Examination*, 4th ed, South-Western Cengage, Mason OH.

Beneish, M. (1997), "Detecting GAAP violation: implications for assessing earnings management among firms with extreme financial performance", *Journal of Accounting and Public Policy*, Vol. 16 No. 3, pp. 271-309.

Beneish, M., Lee, C. and Nichols, D. (2013), "Earnings manipulation and expected returns", *Financial Analysts Journal*, doi: doi.org/10.2469/faj.v69.n2.1.

Block, N. (1969), "Shifting burdens of proof in net worth civil fraud cases", *American Bar Association Journal*, Vol. 55, pp. 688-690.

Casciani, D. (2012), "How Asil nadir stole Polly Peck's millions", *British Broadcasting Corporation*, available at: www.bbc.com/news/uk-19161940 (accessed 16 September 2017).

Comer, M. (2003), *Investigating Corporate Fraud*, Gower, Aldershot.

Calderon, T.G. and Cheh, J.J. (2002), "A roadmap for future neural networks research in auditing and risk assessment", *International Journal of Accounting Information Systems*, Vol. 3 No. 4, pp. 203-236.

Comisky, I. (1981), "The likely source: an unexplored weakness in the net worth method of proof", *University of Miami Law Review*, Vol. 36 No. 1, pp. 1-40.

Dorminey, J.W., Fleming, A.S., Kranacher, M.J. and Riley, R.A. Jr (2010), "Beyond the fraud triangle", *CPA Journal*, Vol. 80 No. 7, pp. 16-23.

Eads, L. (1991), "From Capone to Boesky: Tax evasion, insider trading, and problems of proof", *California Law Review*, Vol. 79 No. 6, pp. 1421-1484.

Han, J. and Camber, M. (2000), *Data Mining Concepts and Techniques*, Morgan Kaufman, San Diego, CA.

Healy, P. and Palepu, K. (2003), "The fall of Enron", *Journal of Economic Perspectives*, Vol. 17 No. 2, pp. 3-26.

Kirkos, F., Spathis, C. and Manolopoulos, Y. (2007), "Data mining techniques for the detection of fraudulent financial statements", *Expert Systems and Application*, doi: 10.1016/j.eswa.2006.02.016.

Kovalerchuk, B., Vityaev, E. and Holtfreter, R. (2007), "Correlation of complex evidence in forensic accounting using data mining", *Journal of Forensic Accounting*, Vol. 3, pp. 1-34.

Lokanan, M.E. (2014), "How senior managers perpetuate accounting fraud? Lessons for fraud examiners from an instructional case", *The Journal of Financial Crime*, Vol. 21 No. 4, pp. 411-423.

Lokanan, M.E. (2015), "Challenges to the fraud triangle: questions on its usefulness", *Accounting Forum*, Vol. 39 No. 3, pp. 201-224.

Manning, G. (2005), *Financial Investigation and Forensic Accounting*, 2nd ed., CRC Press, Boca Raton.

Morales, J., Gendron, Y. and Guénin-Paracini, H. (2014), "The construction of the risky individual and vigilant organization: a genealogy of the fraud triangle", *Accounting, Organizations and Society*, Vol. 39 No. 3, pp. 170-194.

Murphy, P. and Dacin, T. (2011), "Psychological pathways to fraud: understanding and preventing fraud in organizations", *Journal of Business Ethics*, Vol. 101 No. 4, pp. 601-618.

Nigrini, M. (2011), *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations*, John Wiley and Sons, New York, NY.

Simser, J. (2008), "Money laundering and asset cloaking techniques", *Journal of Money Laundering Control*, Vol. 11 No. 1, pp. 15-24.

The Telegraph (2012), "The rise and fall of Asil Nadir's empire", (The Telegraph 22 Aug) [online] available at: www.telegraph.co.uk/news/uknews/crime/9492473/The-rise-and-fall-of-Asil-Nadirs-empire.html (accessed 16 September 2017).

Wells, J. (2013), *Corporate Fraud Handbook*, 4th ed, Wiley and Sons, Hoboken, NJ.

Wells, J. (2014), *Principles of Fraud Examination*, 4th ed, Wiley and Sons, Hoboken, NJ.

Corresponding author
Mark Eshwar Lokanan can be contacted at: mark.lokanan@royalroads.ca