1. Introduction and Background

Polly Peck International (PPI) was a large U.K.-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 Mr. Nadir, PPI used Mr. Nadir’s stock market status in order 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 diversified its operations into consumer electronics, hotel franchises, and fruit and vegetable packaging in Europe, as well as expanded internationally. The expansion and rise in demand for PPI’s product led to a rise in its stock price on the LSE. In 1983, PPI “share price hit a high of £35 before crashing on rumours circulating that the Turkish authorities were about to withdraw tax concessions” (Bowcott, 2010, para. 6) 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 FTSE 100 player (Casciani, 2012, para. 11). In the summer of 1990, there were persistent rumours concerning opaque accounting methods and manipulation of PPI’s share price, which had reached intensity that could no longer be ignored by regulatory authorities, including the Serious Fraud Office (SFO) (The Telegraph, 2012, para. 16).

The Serious Fraud Office (SFO) began investigating PPI in August of 1990 (Nowicka, 1993, para. 1). The SFO initially began investigating Mr. Nadir “by looking at claims of insider dealing - a line of investigation that it later dropped. Instead, it said it found evidence that Nadir had stolen millions of pounds from PPI that belonged to its shareholders” (Casciani, 2012, para. 14). According to media reports, “Nadir exercised an extremely high
level of control over PPI's finances” and “had the power to move money without requiring a counter-signature from another director” (para. 15). For what it is worth, it is important to point out that Mr. Nadir was also both the Chairman and Chief Executive Officer (CEO) of the company when it collapsed (Serious Fraud Office, 2012, para. Para. 7). The company in this sense, suffered from the perennial duality problem associated with corporate governance best practices. The duality problem meant that Mr. Nadir exercised a high degree of control over PPI. As a matter of fact, at trial, the prosecution told the jury that from August 1987 onwards, more than 50 transfers worth about £150m were swindled from PPI accounts (Casciani, 2012, para. 15). Prosecutors went on to claim that

£34m in cash in the 13 specimen charges they put before the jury had been withdrawn in London and moved through other accounts in Switzerland, the Channel Islands, a PPI subsidiary called Unipac and also Kibris, a bank in northern Cyprus controlled by Nadir (Casciani, 2012, para. 15).

During the trial, the court heard 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).

With this brief background in mind, the purpose of this paper is to formulate and propose a fraud investigation plan that forensic accountants can use to investigate the types of activities that occurred at PPI. In particular, the paper will set out the structure and rationale of the fraud investigation plan. The methodology will focus on the accounting manipulation of PPI’s books and the tracing of the proceeds of ill-gotten gains. To gain insight on 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.
1. 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 financial irregularities, which raised suspicion that funds were being transferred from London to other countries and a foreign subsidiary (Casciani, 2012, para. 18; Serious Fraud Office, 2012, para. 8-11). The task is to start with an assessment of the predication that someone from the company 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 the perpetrator behind the fraud 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, in order to develop the context of the case, the following questions are proposed:

- Who is hiding the asset?
- What motivated the individual to hide the asset?
- How did the individual hide the asset?

Developing the context will assist to 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) by key officer(s) of the company.
• Be aware that the stolen funds may flow through various channels.
• Be aware that individuals who are implicated in the fraud may avoid holding assets or accounts in their own name to conceal their role in the fraud.
• Because the key officer(s) of the company may avoid holding asset or accounts in their 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.).
• 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 employ the Bayesian approach (see Srivastava, Mock, & Turner, 2009) and Beneish M-Scores models (Beneish, 1997) 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, Albrecht and Dunn, 2001).

\[ P(B/A) = \frac{P(B/A)}{P(A)} \times \frac{P(A)}{P(B)} \]

Where:

\( B \) = Fraud risk
\( A \) = 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 (\( A \)).
• 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:

\[ P(\text{Fraud risk}|\text{Evidence})=P(\text{Evidence}|\text{Fraud risk})\times P(\text{Evidence}) \times P(\text{Fraud risk})/P(\text{Evidence}) \times P(\text{Fraud risk}) \]
To further filter the information from the initial predication, the investigation team can also employ the Beneish M-Score to test for earnings manipulation. The Beneish M-Score is a mathematical model that is used to analyse whether a company has manipulated its financial statements (Beneish, 1997). The M-Score uses 5-variable and 8-variable financial ratios to test for earnings manipulation in companies’ financial reports. The M-Score formulae are:

5-Variable Model:

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

8-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
- 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, Lee and Nichols, 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 regards to key officer(s) of PPI who may be involved in the fraud, business cards, personal records, Internet
and interviews with associates and acquaintances will be conducted to gather the following information:

- Date of birth, identities of close relatives, friends and business associates
- Their national insurance number, last known address and the names of their 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 these officer(s) have dealt with in the U.K. Special investigative techniques, such as physical surveillance and witness interviews, can be used to keep abreast of their actions and whereabouts. The investigation team may want to obtain authority from the court for civil orders for the CEO 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 their foreign accounts, assets, persons and entities.

2. **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 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 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 strategy 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. These personnel include
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 the perpetrator(s) of the fraud. All of PPI’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. This can be done through a critical evaluation of the data to 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. In the PPI’s case,

[I]t was uncontested that Asil Nadir gave instructions to authorise the movement of funds out of a number of PPI bank accounts; including one with National Westminster Bank and two with Midland Bank. He undertook this on his own signature, without consulting PPI’s board of directors. He had ensured that he retained authority being both chairman and chief executive to do this, applying an autocratic approach to his management style (Serious Fraud Office, 2012, para. 7).

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 funds and assets may have been transferred to foreign entities. 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 to fund the life
styles of key officers of the company.

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 the manner in which they
are been concealed to escape scrutiny. It is expected that the information obtained during the
interviews 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 the PPI’s case, tracing involves
the movement of funds in and out of the London accounts and to find the accounts and
destinations into which the money is being parked (Serious Fraud Office, 2012, para. 8-11).
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 from 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.

3. Models and Methods to Gather and Provide Evidence

The models employed 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. The evidence
gathering process in the investigation is mostly focused on the techniques to gather evidence
of the individual’s criminogenic actions. The conversion aspect of the evidence gathering process focuses on how the fraudster benefited from the proceeds of crime (Albrecht et al., 2012). Based on the evidence from previous behavioural fraud research, the proceeds from stolen funds are sometimes used to fund the individual’s lifestyles (Morales, Gendron and Guénin-Paracini, 2104; Lokanan, 2015). An examination of the spending habits of the individual(s) implicated in the fraud 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 suspect(s) (ACFE, 2014; also see 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 from 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 the suspect’s financial profile: direct and indirect approach.

4.1.2 Direct Approach

The direct approach to tracing stolen funds employs 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 to trace the source of funds. In the present case, the investigation team should focus attention on the following sources to build financial profiles of the key suspect(s): documents from the banks and other financial intermediaries with whom they dealt with. The investigation team may also want to look at tax records (both foreign and local), accounting reports and financial statements of all entities, banks 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 the PPI’s fraud, it is highly likely that direct evidence of the stolen funds may not be available or the investigators will be denied access to 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, 2005; Simser, 2010). The investigation team can use several sources to identify whether the key suspect was living beyond his/her means and build a financial profile. Interviews can be conducted with the key suspect and his or her associates where possible. Close scrutiny should also be on the suspect’s lifestyle, assets (i.e., residence, properties, 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 the suspect and audit reports of the company.

To prepare a financial profile of the suspect, the investigation will follow the following steps for the relevant period. First, identify all assets held by the suspect. Second, identify all of the suspect’s 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 the suspect’s expenses incurred. Fifth, once the investigation team has identified the suspect’s assets, liabilities, income and expenses, and assigned those values, they should have enough data to calculate his or her net worth. While the suspect’s net worth is circumstantial proof, it can be corroborated with testimony of co-conspirators (i.e., the suspect’s bankers, associates, etc.) as circumstantial evidence that he or she stole from the
company. It is expected that the network statement will give investigators a complete financial profile of the suspect's and PPI's operations (see 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 the suspect's and company'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/her net worth (i.e., assets less liabilities) or spent on personal living expenses (e.g., food, rent, 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 of interest to the investigator. To put this into context, since there are suspicions regarding the suspect’s increased net worth, the asset method should be employed to examine whether the suspect has invested illegal funds to accumulate wealth and acquired assets (Adkisson and Riser, 2004; Albrecht et al., 2012; Lokanan, 2014). The expenditure method should be employed to see how the suspect’s lifestyles (for example travels) affect his or her net worth. The increase in the suspect’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.

4.2.1 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 other companies that it conducted business with. Unusual occurrences from operations will become transparent. The business profile is used to provide evidence of the movement of stolen funds from the point of transfer from PPI’s accounts 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. These personnel include the suspect’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 the suspect’s actions. All of PPI’s business records (financial statements and tax returns) should also be reviewed to show its overall financial condition.

4.2.2 Bank Deposit Method

The investigation team should also look at the bank deposit method for potential evidence of the case. They should implement filters and look for round sum amounts (£100,000, £150,000, £200,000, etc.) going out of the account and build and audit trail of those amounts. That is, the investigators should look to detect the accounts and destinations into which the stolen funds were being channelled.

4.2.3 Asset Tracing

Asset tracing is vital to the transportation of the funds. The investigation team should trace assets to see if the funds were used to buy assets in other countries. Asset tracing will provide valuable evidence, which can then be corroborated by investigators (Center for the Advancement of Public Integrity, 2016, p. 1). Asset tracing can also establish new leads for follow-up investigation (p. 1).

4.2.4 Direct Tracing
Assuming that the books and records of PPI are in reasonably good condition and are accessible, direct tracing of funds can be carried out to help the investigation team 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 the 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 (see 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 backwards from summary to origin ensures that the summary figures are based on actual transactions.

4.2.5 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 (see 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, the suspects can leverage their contacts to transfer assets to family members or other related third parties, which will still allow them to
maintain control. They may protect the assets by transferring them and opening children or
family trust accounts or prepay a significant portion of their mortgages on properties (homes),
insurance or credit cards, etc.

4. Conversion Method
4.1 Behavioural Profile

The behavioural profile complements the financial profile and provides possible
motives for the main suspect(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 the
suspect’s behaviour from all accounts stems from singular actions rather than the action of
the collective.

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

5. **DATA Mining Techniques**

6.1 **Benford’s law**

The investigation team should employ 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 funds were being diverted 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 (1) to occur about 30% of the time and integer (2) to occur about 18% of the time. The same logic applies when two digits are used with 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% 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% 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”.

15
6.2 Decision Tree

Another useful data mining technique 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, Spathis and Manolopoulos, 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 of a hypothetical scenario. The diagram depicts a hypothetical case where funds of less than $100,000 are sprinkled to banks and funds of more than $100,000 are sprinkled to family members. Algorithms can then be employed to validate the transactions of the funds from one account to another.
6.3 Artificial Neural Networks

Artificial Neural Networks is a technique used in fraud detection mainly in the context of supervised classifications (Calderon and Cheh, 2002). Neural Networks is a datamining 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 signals (Kirkos et al., 2007, p. 999). When the combined input signals are 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:
where:

\[ ub = Rwib \times xi \]

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

**Figure 3: Neural Network Algorithm**

6.4 *Goodness-of-Fit-Test*

The chi-Square Goodness-of-Fit-Test can also be used to detect 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.

6. Recommendation for the Investigation

To determine the factual basis of the allegations of fraud, the investigation team should first use the data collected and build a personal and financial profile of the main suspect(s) 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 other countries. The stolen funds may change form as they flow through various channels orchestrated by the suspect(s) (see ACFE, 2014, p. 25). The suspect(s) may also try to avoid transferring the accounts into funds that are in their names; 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 a financial profile of the suspect(s). The direct method approach to the suspect’s financial standing and profile should be triangulated with the direct method of asset tracing. It is assumed that, as a publicly traded corporation, the books and records (or at least some of them) of the suspect(s) and PPI are in reasonable good order and, as such, direct tracing of transactions and funds through the business, or through a person’s hands, may be possible (see also Kovalerchuk, Vityaev and Holtfreter, 2007; Lokanan, 2014). Due to endless audit trails and paper transactions, corporate fraud can take a long time to plan and execute (Albrecht et al., 2000; Adkisson and Riser, 2004). 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 the suspect’s receipts and his or her subsequent disposition of funds (see also ACFE, 2014, p. 32). The investigation team should also triangulate the indirect method of building the suspect’s net worth with the indirect method of asset tracing. These various indirect methods are employed to detect whether the suspect(s) was able to accumulate funds that did not come from legitimate sources. Together, the indirect method to build the suspect(s) financial profile and the indirect approach to tracing their assets can give investigators a good idea of the their net worth. The indirect approach should also be triangulated with the suspect(s) behavioural profiles. This will assist investigators to analyse whether the stolen funds were either spent on lavish lifestyle purchases or were 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 the suspect’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


