Utilising advanced accounting software
to trace the reintegration of proceeds of crime,
from underground banking into the formal banking system

by

Christo Botes

submitted in part fulfilment of the requirements
for the degree of

MAGISTER TECHNOLOGIAE

In the subject

FORENSIC INVESTIGATION

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: DR NJC OLIVIER

APRIL 2008

STATEMENT OF OWN WORK
Student number 3725-289-5

I, Mr Christo Botes hereby confirm that my Masters Degree thesis titled:

"Utilising advanced accounting software
to trace the reintegration of proceeds of crime,
from underground banking into the formal banking system"

was researched, compiled and drafted by myself and is indeed my own work.

_____

Mr Christo Botes.

Signed at, Centurion, South Africa, 20 January 2009.

AKNOWLEDGEMENTS

There are many people I would like to thank for helping me to make this project a success.

First of all, I would like to thank my mentor and supervisor, Dr Nick Olivier. Your guidance, wisdom and patience over the past five years are a direct contribution to the success of this master's degree. We travelled this road together but your wisdom steered the ship.

Also, my wife Charmaine, thank you for your support, understanding and patience.

To Mrs Susan van Tonder, for editing the dissertation, your help came at the right time.

And lastly, a great big thanks to all the respondents taking part in the very interesting project. You all are professionals and you gave me your most valuable asset, time.

Your time directly contributed to the quality and success of this master's degree.

ABSTRACT

The aim of this paper is to research how advanced accounting software can be used by police detectives, financial risk specialists and forensic investigation specialists, who are responsible for the investigation and tracing of the reintegration of proceeds of crime, from underground banking into formal banking system (pro active and reactive money laundering investigation) with a view on criminal prosecution.

The research started of by looking at the basic ways how proceeds of crime are smuggled before it is integrated into the formal banking system. In that context, the phenomenon of Underground banking was researched. Currency smuggling, Hawala currency transfer schemes and the way in which it is used to move proceeds of crime were discussed in detail. Thereafter Formal banking and the way in which proceeds of crime is reintegrated from underground banking structures into formal banking systems were discussed.

The use of advanced accounting software to trace the point where proceeds of crime are reintegrated into formal banking were researched extensively. Accounting software and investigative techniques on how to trace financial transactions which might be tainted with proceeds of crime were discussed. Accounting software which can be used on office computers such as laptops were discussed and more advanced automated systems which can be used to trace proceeds of crime transactions in the formal banking systems were also discussed. In specific, the investigative techniques on how to use these systems as investigative tools were discussed in great detail. This research paper gives a truly unique perspective on the financial investigative and analytical angle on proceeds of crime and money laundering detection.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AML	Anti-money laundering, the process by which efforts are made to prevent and detect money laundering activity (KPMG, 2007:15).
FIU	A Financial Intelligence Unit is a central, national agency responsible for receiving (and as permitted, requesting), analyzing, and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to combat money laundering and terrorism financing (KPMG, 2007:16).
FATF	The Financial Action Task Force is an intergovernmental body. Its Secretariat is based at the Organisation for Economic Co-operation and Development (OECD). Its purpose is to develop and promote policies to combat money laundering and terrorist financing. It has thirty-three member countries (KPMG, 2007:16).
FINCEN	Financial Crimes Enforcement Network, the network established by the U.S. Department of the Treasury in 1990 to support federal, state, local, and international law enforcement by analysing the information required under the Bank Secrecy Act, and by enhancing information sharing between these bodies (KPMG, 2007:16).
KYC	Know Your Customer, the requirement that financial institutions understand who their customers are, which includes obtaining documentation to verify identity, address, source of funds etc (KPMG, 2007:16).

OFAC The Office of Foreign Assets Control ("OFAC") is part of the United States Department of the Treasury. It administers and enforces economic and trade sanctions against targeted foreign countries, terrorists, international drug traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction (KPMG, 2007:18).

PEPs Politically Exposed Persons refers to persons who perform important public functions for a state and includes, heads of state, government and cabinet ministers; senior judges; senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organizations; and members of ruling royal families. The term also applies to the family and close associates of such individuals (KPMG, 2007:18).

STR/SAR Financial institutions must submit a Suspicious Activity Report to law enforcement/regulatory authorities when they have a suspicion that transactions involve funds derived from criminal activity, are intended to hide or disguise funds derived from criminal activity (money laundering), or are being structured to evade reporting requirements (e.g. those under the United States Bank Secrecy Act) (KPMG, 2007:18).

CHAPTER 1:
GENERAL ORIENTATION

1.1 INTRODUCTION

The government and major companies are now compelled by law to implement certain counter measures to identify, prevent and report suspicious transactions, currency smuggling, and money laundering activities. The concerns by the banking sector and law enforcement are how to comply with the new legislation and how to identify proceeds of crime when it enters the formal banking system. On the other hand, if trained financial people have difficulty in tracing the reintegration of proceeds of crime from underground banking into the formal banking systems, how will police officers and forensic professionals investigate and prosecute the reintegration of proceeds of crime into formal banking systems?

Finance Minister Trevor Manuel has said that US $ 2 billion to US $ 8 billion in dirty money may be laundered through South Africa's financial institutions every year, a not insignificant share of the estimated US $ 600 billion believed to be laundered globally each year (Michell, 2005:40). The phenomena of underground banking and the reintegration of proceeds of crime from underground banking into formal banking systems are seen in such a serious light that in South Africa these type of financial activities are prohibited and punishable by at least four different pieces of legislation and can carry a sentence of 30 years imprisonment or a fine of R 100 million, in terms of section 4 of the Prevention of Organised Crime Act 121 of 1998 POCA (South Africa, 1998). There are attempts by certain institutions to train law enforcement agencies in the identification of proceeds of crime in underground banking and the reintegration thereof into the formal banking system, but the insight offered by this training is vague, superficial and not well researched.

1.2 RESEARCH AIM

The aim of this report is to research how advanced accounting software can be used by police detectives, financial risk specialists and forensic investigation specialists, who are responsible for the investigation and tracing of the reintegration of proceeds of crime from underground banking into formal banking systems (pro-active and reactive money laundering investigation), with a view to criminal prosecution.

1.3 RESEARCH PURPOSE

There must be a reason for doing research as otherwise there would be no point to spending time, money and effort undertaking the investigation (Denscombe, 2002:25). With this in mind, the researcher decided to look at the problems surrounding a string of recent convictions of banks for money laundering offences, such as the Royal Bank of Scotland, which was fined £ 1,250,000.00 million during January 2004 (Cliffe, 2004:2), and ABN AMRO Bank, which was fined US $ 80 million during December 2005 (Gormley, 2005:3). These fines raised serious questions about the systems and best practice banks around the world utilise to curb money laundering.

The main driving force behind a piece of research is sometimes the desire to solve a practical problem or to improve procedures (Denscombe, 2002:25). Particularly in the context of organisations and the work environment, the aim of a research study is to arrive at recommendations for good practice that will tackle a problem or enhance the performance of the organisation and individuals through changes to the rules and procedures within which they operate (Denscombe, 2002:25).

This research evaluated the strengths and shortcomings of the current Anti Money Laundering (AML) accounting and investigative systems. The purpose of the research was to find the most effective technique for identifying and investigating the flow of proceeds of crime and money laundering transactions through a banking system.

The research achieved this purpose through exploring national and international literature, with a specific focus on highly regulated banking environments such as South Africa, and with some references to incidents in the United States of America and the United Kingdom. However, the geographical area of the research focused on the Gauteng area of South Africa.

The researcher wanted to arrive at recommendations for good practice with regard to the use of AML investigative systems, which would shed new light on the use of advanced accounting software in the fight against money laundering. This research will benefit police detectives involved in reactive money laundering investigations and bankers involved in pro-active identification of money laundering transactions.

1.4 RESEARCH QUESTIONS

Research questions of a research study specify exactly what is to be investigated. They are not the broad goals of the research that are directly investigated by the research – specific things that are to be observed, measured, and interrogated in order to shed light on the broader topic. Research questions express the basis for the design (Denscombe, 2002:31).

To address the research problem, the researcher developed the following research questions to be answered during the research:

1.4.1 What is the difference between underground banking and formal banking systems?

1.4.2 What type of advanced accounting software can be used to trace the reintegration of proceeds of crime from underground banking into the formal banking systems?

1.4.3 Which advanced accounting software systems can be used as an investigative technique in tracing the reintegration of proceeds of crime from underground banking into the formal banking systems?

1.5 KEY CONCEPTS

The researcher included a list of definitions to explain certain terms that are used in the research report. This was necessary because some of the literature collected refers to some very uncommon and technical terms, which will not be understood at first reading without explanation.

1.5.1 AML systems (AML investigative systems)

Anti Money Laundering (AML) software can be described as the use of advanced algorithms to identify money laundering transactions (Lee, 2002:1).

1.5.2 Hawala

In the Urdu language, “hawala” means “reference”, while in Arabic it means “transfer”. Consequently, formal bank transfers are conducted in “hawala departments in parts of the Arab world”. It is more accurate, therefore, to separate formal from informal hawala (Passas, 2003:2).

1.5.3 Proceeds of unlawful activities (proceeds of crime)

“Proceeds of unlawful activities” are “any property or any service, advantage, benefit, or reward which was derived, received, or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act [Prevention of Organised Crime Act], in connection with or as a result of any unlawful activity carried on by any person, and

includes any property representing property so derived" (POCA Act, 1998:2).

1.5.4 IVTS (Informal Value Transfer Systems)

"IVTS" refers to any network or mechanism that can be used to transfer funds or value from place to place either without leaving a formal paper trail of the entire transaction or without going through regulated financial institutions (Passas, 2003:12).

1.5.5 Underground banking

"Underground banking" is a generic term used to describe any informal banking arrangement which runs parallel to, but is generally independent of, the formal banking system (McCusker, 2005:1). Underground banking systems are also referred to as "alternative remittance systems" by the Financial Action Task Force (FATF) (McCusker, 2005:1); "informal funds transfer systems" (World Bank & International Monetary Fund) (McCusker, 2005:1); and "informal value transfer systems (IVTS)" by the US Financial Crimes Enforcement Network – (FINCEN) (McCusker, 2005:1).

1.6 RESEARCH APPROACH AND DESIGN

To get to the bottom of the problem one is investigating, one needs to get answers from practice. For this reason, the researcher made use of the empirical research design, because, according to Babbie (1998:4), empirical research is the production of knowledge based on experience or observation. The researcher conducted interviews with police detectives, and banking and forensic audit professionals, in which their conclusions were based on experience. Empirical research is one way of knowing things about crime and criminal justice. Another reason for using the design is that, as an approach to social research, the emphasis in the empirical design tends to be on producing data based on real-world observations. The very notion of this research is that the

research has involved an active attempt by the researcher to go out and look and search (Denscombe, 2002:27).

This type of research is associated with getting information 'straight from the horse's mouth'. The research is also purposeful and constructed (Denscombe, 2002:27).

The approach that the researcher followed is a qualitative approach. The researcher considered this to be the best choice of approach because a qualitative approach can involve existing data and historical research, which is very often used in the field of law and criminology (Welman & Kruger, 1999:186). The approach adopted in the study focused on locating existing documents; for example, books, newspaper reports, official statistics, law reports and Internet articles.

The procedures used have been designed to provide outsiders with maximum insight into the situation being investigated. Qualitative research involves a series of research techniques where the researcher has direct and sustained social interaction with participants in a particular setting (Mouton, 2001:208).

1.7 TARGET POPULATION AND SAMPLING

The target population is the population about which the researcher ideally would like to generalise in his work (Welman & Kruger, 1999:122). The population of a research study includes all individuals or cases of a certain type (Welman & Kruger, 1999:122). In this case, the population involves about 95 AML practitioners that have knowledge within the field of AML investigations. These practitioners are all working for the South African Police Service (SAPS) and companies which are involved in money laundering investigations. There are about 14 organisations, including the SAPS, handling these investigations. A selection was made from this list of companies,

banks, audit firms and the units of the South African Police Service (SAPS).

The selection of companies was made by drafting a list of all 14 organisations, including the SAPS, and then allocating a number to each company in a random order. A sample from a list containing only numbers, which were representative of the organisations, was selected by randomly pointing a pencil at the numbers on this list. A selection of seven organisations was made.

The seven organisations selected included: the SAPS Commercial Crime Unit, the Organised Crime Unit of the SAPS, Standard Bank Ltd, Johannesburg Stock Exchange, Deutsche Bank Ltd, PricewaterhouseCoopers Forensic Accounting, Moneygram International Ltd, and a Consulting Chartered Accountant of South Africa (CASA).

Thereafter, a name list was obtained from each organisation, which was used for further selection of names within those organisations.

To select the sample of 30 respondents, a first list was drafted, containing all the names received from private sector companies, from banks and from audit firms. This list did not include police members. In this list, each name was allocated a random number. A selection was made from a list containing only random numbers, which represented these names. Random sampling was used to select the respondents by randomly pointing a pencil at the numbers on this list and marking the number selected. Through this technique a selection of six private sector respondents was made, which included: respondents from forensic audit firms and banking, such as Standard Bank Ltd (1), the Johannesburg Stock Exchange (1), Deutsche Bank Ltd (1), PricewaterhouseCoopers Forensic Accounting (1), Moneygram International Ltd (1), and a Consulting Chartered Accountant of South Africa (CASA) (1). It must be noted that the respondents mentioned

above are not police investigators. They are private sector financial risk specialists, such as Chartered Accountants (CA) and bankers involved in the monitoring and investigation of all financial risks such as fraud and money laundering within their organisations.

A second list, containing the names received from the SAPS Commercial Crime and Organised Crime units, was drafted. This list contained the biggest number of people and was much larger than the other list (private sector list); as a result more people were selected from this police officer list. In this second list, each police detective's name was allocated a random number. The simple random sampling technique was again used to select respondents. A selection was made from a list containing only random numbers, which represented the names of the police detectives. This was done by randomly pointing a pencil at this list and marking the number selected. In this way a selection of 24 police detectives was made from this list. These respondents are from the SAPS Commercial Crime and Organised Crime units.

Permission to interview the above-mentioned respondents was sought from their employers. In particular, in terms of *Research in the Police Service*, *National Instruction 1/2006,* the Assistant-Commissioner, Head Strategic Management, in the Strategic Management Division of the SAPS issued an authorisation letter, which authorised the researcher to interview the respondents.

In summary, the researcher selected a sample from the target population, and identified a sample of 30 respondents from the comprehensive sampling frame. The researcher made use of a probability sample and, in particular, used random sampling, to select the sample. According to Kruger and Welman (1999:55), the advantage of a simple random sample is that it is representative of the population.

1.8 DATA COLLECTION

Mouton (2001:69) describes primary data as an information source/data, whether the researcher has to collect it himself or whether it already exists in one form or another. Primary data is usually available in one of two forms: textual information or numeric information or data. The researcher made use of primary and secondary data, because these sorts of data supported most of the interviews with AML practitioners. Mouton (2001:69) describes secondary data as written sources (including the Internet), which discuss, comment, debate, and interpret primary sources of information. The interviews conducted with the respondents made provision for secondary data in that they allowed those respondents who wished it to attach systems' documents, annual reports etc. as examples and/or annexures.

The data-collection techniques outlined below were used during the research process.

1.8.1 Literature

The researcher followed Mouton's (2001:90) tips for effective reading of literature, such as reading most recent works first and then working one's way back to less recent sources; reading abstracts or summaries of an article first before starting to read the whole article; looking for articles with clear introductory sections; and, lastly, once the researcher had discovered that a book or other source was relevant, reading the source in depth and systematically.

The researcher could not locate literature on exactly the same topic as the research study during the literature review. Other access points were also searched, such as Google, Bookfind, WorldCat, SAMedia. Dispersed Internet articles on banking risk software were located, but did not have titles relating to the area of the research study. However, the researcher did locate literature that focused on proceeds of crime

and the legal discussions surrounding it. These books ponder legal theories of proceeds of crime and procedures of court actions. They do not fully address the research area; however, some aspects were relevant. The researcher's study is about the investigative tool of advanced accounting software, which is used to trace proceeds of crime and money laundering transactions into formal banking systems.

The literature collected can be considered to be valid because it was collected from a wide range of sources and the researcher followed Mouton's (2001:90) criteria for a good literature review:

- The literature review was exhaustive in what it covered, and literature was collected from books and journal articles to Internet sources and news paper articles;
- The literature review was fair in its treatment of authors, and the researcher objectively reviewed and analysed a range of authors' papers;
- The literature review was topical and not dated;
- The literature review was not only confined to Internet resources; and
- The researcher made sure that the literature review was very well organised.

The researcher studied this literature to find answers to the questions included in the interview schedules, which he had drawn up on the basis of the research questions.

1.8.2 Interviews

The study used structured interviews as a way of collecting data, as described by Kruger and Welman (1999:166). In a structured interview, the interviewer puts together a collection of smaller questions that are derived from the research questions and aims of the research. This is known as the interview schedule, and the respondents' responses are noted by the researcher as the questions are put to them.

These structured interviews were used because very specific questions on the use of advanced accounting software and artificial intelligence-based AML software to monitor financial transactions were asked with the aim of eliciting descriptions from the respondents.

Leedy and Ormrod's (2001:159) guidelines for conducting productive interviews were followed by the researcher as follows:

- The researcher sought written permission from the various respondents' employers, and interviews were conducted with the respondents;
- The researcher found a suitable location, normally after hours, in which to conduct the interviews;
- The researcher took a few minutes to establish rapport in order to make the respondent feel comfortable;
- The researcher did not put words in the respondents' mouths and allowed them to discuss and elaborate on any answer as they deemed necessary;
- The researcher recorded the respondents' responses *verbatim* in a written document (interview schedule) as interview notes (field notes);
- The researcher kept his reactions to himself and never showed surprise or disapproval;
- The researcher always remembered that the facts are not necessarily portrayed, and always treated the respondents' responses as *perceptions* rather than as the facts.

1.8.3 Documents

Documentary sources may be defined loosely as records relating to individuals or groups of individuals (Miller & Brewer, 2003:80). Several documents relating to the AML environment were also located from the Financial Intelligence Centre of South Africa. Very relevant statistics of Suspicious Transaction Reports (STR) from 2003 to 2006 were used in

the research. These statistics cover all STRs made by registered banks in South Africa.

Also, the researcher located actual legal papers from the United States Financial Crimes Enforcement Network (FINCEN), which described legal proceedings against and fines given to several of the world's biggest banks for money laundering offences. Similar legal documents from the United Kingdom's Financial Services Authority (FSA), outlining money laundering breaches by one of the United Kingdom's biggest banks and the banks involvement, were located.

The researcher used these documents (and made appropriate referencing) to critically analyse the formal banking procedures in place to curb money laundering. Documents were also used to discuss what action and fines were being imposed on banks for major money laundering breaches. Lastly, they were used to discuss and explain the type of advanced accounting software (AML systems) which is available for the pro-active curbing of money laundering in a formal banking environment. All the documents were dealt with in the same way.

1.9 METHOD OF DATA ANALYSIS

In analysing the research data, the researcher begins with a large body of information and must, through inductive reasoning, sort and categorise it, and gradually boil it down to a small set of abstract, underlying themes (Leedy & Ormrod, 2001:160). The researcher made use of the data analysis spiral, which is applicable to a wide variety of qualitative studies, as explained by Leedy and Ormrod (2001:161). This process entails using raw data to form the basis of one's research study by carrying out the steps outlined below.

1.9.1 Organisation

The researcher set up a filing scheme, which contained research proposal correspondence and a section for research notes, subdivided into software research, AML research papers, and several other sub-sections that allowed the researcher to break larger sections of information into smaller ones. A backup of all the information was also created on the researcher's laptop, with similar folders, also containing two databases on currency smuggling and banking AML software usage. The research was organised within this framework.

1.9.2 Perusal

All the information was perused several times and relevant data was noted and extracted by making use of markers and personal notes.

1.9.3 Classification

The researcher categorised the data into smaller groups and themes. For instance, the researcher created electronic folders dividing banking AML software into international (other countries and banks) and South African banks and divided these folders into two groups. Several other themes were sub-structured in this way. This gave the researcher a clear idea of what the data meant.

1.9.4 Synthesis

At the synthesis stage, the researcher integrated and summarised the data. This step included offering propositions or hypotheses that described relationships among the categories (Leedy & Ormrod, 2001:161).

1.9.5 Final report

The final report was finalised into chapters and headings within these chapters, each of which addressed a research question.

1.10 METHODS TAKEN TO ENSURE VALIDITY

Validity concerns the accuracy of the questions asked, the data collected and the explanations offered in a research investigation. Generally, it relates to the data and the analysis used in the research (Denscombe, 2002:100). The questions asked were valid because they were based on the research questions.

The researcher regards the data-collection techniques that were used as valid on the basis of the factors described below:

1.10.1 Validity of interviews

The interview schedule was divided into sub-sections directly related to the original research questions, which in turn sought to address the main working title of the research report.

There were no factors influencing the actual interviews and the way they were conducted; the respondents were interviewed in a normal environment, and pre-arranged meeting dates were set up. The respondents approached the interviews as passive, neutral beings (Welman & Kruger, 1999:109). There was no reactivity of research; there was no placebo effect, no Hawthorn effect, and no John Henry effect, and no demand characteristics were noticed during the interview process, as pointed out by Welman and Kruger (1999:109).

In addition, the guidelines for conducting productive interviews, as pointed out by Leedy and Ormrod (2001:159), were followed.

1.10.2 Validity of literature

The literature collected may be considered to be valid because it was collected from a wide range of sources, and the researcher followed Mouton's (2001:90) criteria for a good literature review.

1.10.3 Validity of documents

The documents located were also valid because the fact that the researcher read competing or rival hypotheses shows that the researcher reviewed all literature objectively. Legal documents describing court proceedings against banks or fines imposed on banks have a lot of validity in themselves because their content is likely to have been critically analysed, objectively argued about in court, and had decisions made on it by legal practitioners.

The researcher can argue that the fact that the documents were drafted and processed by attorneys substantiates the validity of the documents. The process in itself substantiates the relevance and validity of the documents. Relevance, authenticity and validity are some of the underlying legal principles of acceptance of documents in court proceedings.

Also, the use of descriptive AML investigative systems documents that are currently in use and implemented by banks to curb money laundering should be accepted as valid. These documents have been used in the research, design, testing and implementation of AML investigative systems for several major banks in South Africa and around the world. This is likely to prove the documents to be valid because, as Denscombe (2002:100) states, the researcher can argue that their findings are better than common sense or casual investigation.

1.10.4 Validity of data analysis

The data analysis was valid because the researcher adopted a structured, chronological approach to data collection and analysis from the start of the research project. This ensured that no mistakes were made with the initial data-collection process and also had the direct effect of a valid and reliable data-analysis process.

The researcher followed Leedy and Ormrod's (2001:161) data-analysis spiral process. Their approach to data collection and analysis, as described above (see 1.9.1 to 1.9.5), and Mouton's (2001:109) data-capturing guidance were adhered to and the researcher ensured that:

- No data-capturing errors occurred during the data-collection process and the researcher captured the data himself, captured the data manually and point by point, and saved a master copy in an archived data folder, to ensure that original data-capturing records stayed constant;
- No post-coding errors occurred after data collection because the researcher referred back to chronologically filed documents and field notes and interview schedules. The researcher did all the data capturing himself and re-checked the data capturing several times;
- No missing values during data capturing involving statistics could be identified and all statistical values were captured manually and point by point by the researcher; each value was also re-checked and compared to totals. This process eliminated any capturing or coding errors.

In this way, the researcher ensured that no errors or omissions were made during the data-collection process that would have an effect on the validity of the data.

Adding to the above, Mouton's (2001:110) data-analysis interpretation (synthesis) guidance was also integrated into the data-analysis system of checks, with the researcher taking care not to draw inferences from data that were not supported by the data and not to be biased in interpretation of data through selectivity.

1.11 METHODS TAKEN TO ENSURE RELIABILITY

Reliability relates to the methods of data collection and the concern that these should be consistent and not distort the findings. Generally reliability entails an evaluation of the methods and techniques used to collect the data (Denscombe, 2002:100).

The researcher regards the methods of data collection as reliable because they will not vary from occasion to occasion. For example, if the researcher were to interview two respondents about the use of the "FORTENT AML system", the same results would be achieved because the method would produce the same result. However, the researcher put all measures in place to ensure internal consistency, where he sought a high degree of generalisation across the items within the measurement (Welman & Kruger, 1999:144).

1.12 ETHICAL CONSIDERATIONS

Leedy and Ormrod (2005:101) are of the view that, whenever human beings are the focus of investigations, researchers must look closely at the ethical implications of what they are proposing to do. Most ethical research falls into one of four categories: protecting from harm, informed consent, right to privacy, and honesty with professional colleagues (Leedy & Ormrod, 2005:101). Denscombe (2002:165) refers to "ethics" as: (a) the duties and responsibilities of individuals; with (b) broader systems of moral principles and rules of conduct. Ethics concerns the system of moral principles by which individuals can

judge their actions as right or wrong, good or bad. This means that the ultimate goal of science is the search for truth (Mouton, 2001:239).

The researcher realises the limitations of the research and confirms that the field of research was very technical, as money laundering is the most sophisticated area of organised crime. However, the adherence to ethical research translates into a number of rules or conventions, which were integral to the research process.

The researcher took into consideration issues such as: objectivity and integrity in research, no fabrication or falsification of data, recording of own data, ethical publishing practices, appropriate ascription of authorships to a publication, rejection of any form of plagiarism, no simultaneous submission of manuscripts, no secret or clandestine research, an obligation to the free and open dissemination of research results, the right to privacy, the right to anonymity and confidentiality, and the right to full disclosure about the research (Mouton, 2001:239-245).

With regard to the right to privacy, Mouton (2001:239) believes that the researcher has the right to search for truth, but not at the expense of the rights of other individuals in society. Under no circumstances should a research report, either oral or written, be presented in such a way that others become aware of how a particular participant has responded or behaved (unless the participant has specifically granted permission, in writing, for this to happen) (Leedy & Ormrod, 2005:102). In general, a researcher must keep the nature and quality of a respondent's performance strictly confidential (Leedy & Ormrod, 2005:102).

The researcher adhered to Mouton's (2001:243) guidance on the right to privacy (including the right to refuse to participate in research) and followed the guidelines mentioned by Mouton. Researchers, for example, have the right to collect data through interviewing people, but

not at the expense of the interviewee's right to privacy (Mouton, 2001:239).

With regard to protection from harm during research, Mouton's (2001:245) guidelines were followed and the researcher ensured that no respondent was subjected to substantial risk of personal harm. Leedy and Ormrod (2005:102) also state, with respect to protection from harm, that a researcher should not expose research respondents to undue physical or psychological harm. No intrusive measures, such as physiological or psychological experiments, situations involving abnormal stressful stimulus or activity, or procedures involving the dosing of respondents, were used during the research, as guided by Mouton (2001:245).

The researcher followed Mouton's (2001:243) ethical guidelines and did not force people to be interviewed, and adhered to their right to refuse to be interviewed. He also acknowledged people's rights to refuse to answer any questions. The researcher did not interview respondents at mealtimes, at night, or for long periods.

With regard to informed consent, respondents should be told the nature of the study to be conducted and given the choice of either participating or not participating (Leedy & Ormrod, 2005:101). Furthermore, the respondents were notified that they had the right to withdraw at any stage even if they had agreed to participate (Leedy & Ormrod, 2005:101). Any participation in a study should be strictly voluntary (Leedy & Ormrod, 2005:101).

In following Mouton's (2001:244) guidelines, the researcher communicated which institution he represented, the aims of the research, rights in terms of anonymity, and how the data would be used and disclosed as part of the research report.

Honesty and professionalism with colleagues is taken into consideration and, in terms of Leedy and Ormrod's (2005:102) guidance, the researcher reported findings in a complete and honest fashion, without misrepresenting what was done or intentionally misleading others about the nature of the findings (Leedy & Ormrod, 2005:102).

1.13 RESEARCH STRUCTURE (CHAPTERS AND LAYOUT)

The research structure consists of five chapters and the layout is as set out below.

1.13.1 Chapter 2: Banking Systems

In this chapter, the research takes an in-depth look at the so called phenomenon of underground banking and its interaction with formal banking. In particular, the occurrence of underground banking techniques, such as currency smuggling and "the hawala system," and how these techniques are used to launder dirty money are discussed in this chapter in detail. Also, the convergence, or reintegration, of underground banking money and how it is integrated into the formal banking systems is discussed in a lead up to the use of advanced accounting software systems (AML systems), in the formal banking environment.

1.13.2 Chapter 3: Advanced Accounting Software Systems

This chapter takes a look at what type of advanced accounting software is available for use by the police detectives from the SAPS Commercial Crime and Organised Crime units in reactively investigating money laundering in terms of section 4 of the Prevention of Organised Crime Act 121 of 1998. The research also takes a look at what type of advanced accounting software (AML systems) is available for private sector and financial services institutions, such as forensic audit firms, and the formal banking institutions, such as investment and

retail banks, to identify and report money laundering transactions pro-actively in terms of section 29, of the Financial Intelligence Centre Act 38 of 2001.

1.13.3 Chapter 4: Utilising Advanced Accounting Software to trace Proceeds of Crime Transactions in Bank Accounts

This chapter discusses in detail how advanced accounting software is used most effectively as an investigative tool in financial investigations. It explores advanced functions that can assist in detecting proceeds of crime and money laundering transactions flowing through the formal banking systems. This chapter also discusses real-time transaction filtering and automated AML systems which can be used by banks to detect suspicious transactions such as proceeds of crime and money laundering transactions.

1.13.4 Chapter 5: Findings and Recommendations

This last chapter reaches findings on the basis of the literature reviewed, interviews conducted, and documents collected during the research process. Here, certain recommendations are also made.

CHAPTER 2:
BANKING SYSTEMS

2.1 INTRODUCTION

The banking system is daily at risk of accepting and facilitating the transfer of proceeds of crime transactions. Proceeds of crime and money laundering transactions are very complex and sophisticated and are not easy to detect. The whole essence of money laundering is to hide and conceal dirty money and to change its appearance, from an illegitimate source, to appear as legitimately obtained money (POCA Act, 1998:6).

Goredema (2003:206) states that money laundering in the sub-region of southern Africa occurs on a significant scale; statistics often cited abroad are based on the results of the Walker model. According to this model, in 1998 a total of US $ 22 billion was laundered through the financial systems of southern Africa (Goredema, 2003:206).

Table 2.1 below gives an estimate of the magnitude of money laundering activity in the southern African sub-region. The total amount laundered internally and brought into the eastern and southern areas of Africa during 1999 was equal to or just over US $ 18,07 billion (Goredema, 2003:206).

Table 2.1: Money laundering estimates

Amounts in US $ Millions								
Country	Internal	Outgoing	Total Generated	Incoming	Total laundered	% Internal	% Outgoing	% Incoming
Botswana	123.4	117.6	241.0	1722	1845.0	51.2	48.8	93.3
Kenya	734.8	140.0	874.8	77	811.8	84.0	16.0	9.5
Lesotho	0.9	0.1	1.0	458	458.7	86.4	13.6	99.8
Malawi	96.4	47.0	143.4	62	158.1	67.2	32.8	39.1
Mauritius	95.2	61.4	156.6	1129	1224.5	60.8	39.2	92.2
Mozambique	87.6	34.1	121.7	17	104.8	72.0	28.0	16.4
Namibia	114.6	84.3	198.9	489	603.5	57.6	42.4	81.0
Seychelles	68.1	4.8	73.0	1963	2031.5	93.4	6.6	96.6
South Africa	6143.7	4095.8	10239.5	566	6709.9	60.0	40.0	8.4
Swaziland	20.3	3.2	23.5	414	434.8	86.4	13.6	95.3
Tanzania	693.5	124.3	817.8	63	756.7	84.8	15.2	8.3
Uganda	611.4	130.6	742.0	54	665.9	82.4	17.6	8.2
Zambia	1098.0	427.0	1525.0	177	1274.6	72	28.0	13.9
Zimbabwe	726.6	354.7	1081.3	272	999.1	67.2	32.8	27.3

Source: Goredema (2003:206)

2.2 FORENSIC INVESTIGATION

It is important to explain the relevance of forensic investigation in the context of the above-mentioned cycles, which involve money laundering. This is necessary, because money laundering involves complex financial analysis and financial legal structures. A proper forensic investigative methodology is critical in the investigative approach to such high-level money laundering and proceeds of crime forensic investigation. It is therefore relevant and appropriate to define forensic investigation adequately, with specific reference to a financial forensic investigation.

The forensic investigation process is creating an environment that encourages the detection and prevention of criminal activity. The skills of a forensic investigator are in some respects similar to those of an auditor (Bologna, 1995:29). An auditor and a forensic investigator both seek the truth, the auditor with respect to proper accounting of business transactions and the forensic investigator with respect to the proper (legal) behaviour of citizens. Both should have inquisitive minds

and challenge things that appear out of order and out of sequence, such as odd times, odd places, and odd people – in a word, things that are *opposite* of what one would logically expect (Bologna, 1995:32).

The process of forensic investigation is intended to uncover material deviations and variances from standards of acceptable accounting and auditing used in basic business practices (Bologna, 1995:32). It is also intended to uproot criminal activity and to follow clues regarding *modus operandi* followed in the commission of crimes, to apply the set *modus operandi* followed in the mentioned crime, and to follow trends and patterns in order to identify more crimes committed, with the intention of linking the chain of evidence regarding the crime (Bologna, 1995:32).

For these reasons, the forensic investigative process aims to incorporate proper financial analysis, seeking documentary evidence of proper accounting/business transactions and following proper legal process (Bologna, 1995:32).

The goals of forensic investigation are to identify the perpetrator of the criminal offence, to collect the correct (relevant) evidence in a case against an accused, to prepare a proper case file which can be used in a court of law, and to assist in further investigation and prosecution of the suspects that have been identified (Respondent 19, 2007).

The most important element, identification, is integral to a forensic investigation. Identification (individualisation) relies on uniqueness (**Hoogstrate, Van Den Heuvel & Huyben**, 2000:2). The identification and individualisation of an impression (or other piece of physical evidence) is established by finding agreement between corresponding individual characteristics of such number and significance to preclude the possibility (or probability) of their having occurred by mere coincidence, and by establishing that there is no difference that cannot be accounted for (**Hoogstrate, Van Den Heuvel & Huyben**, 2000:2).

It is imperative to include a clear identification process in the investigative methodology. This process should allow the investigator to correctly identify the perpetrator and relevant evidence for submission in court.

With this in mind, the process of identifying and investigating proceeds of crime within underground banking is discussed below.

2.3 UNDERGROUND BANKING AND FORMAL BANKING

Underground banking has long been regarded as a conduit for money laundering by criminal organisations and arguably by terrorist networks (McCusker, 2005:1). According to Maimbo (2003:8), money laundering occurs in two areas of the economy: the formal economy and the informal economy. Both of these economies have the potential of being misused for money laundering and hiding the proceeds of crime (Maimbo, 2003:8).

It is the unknown area of the underground economy, a grey area, which the research identified as the starting point of many organised money laundering schemes. At that point, any form of proceeds of crime can switch hands; whether it is drug-dealing money, bribery money or prostitution money, no one will know. Criminals who commit offences which generate cash proceeds, for instance cash heists or drug trafficking, are often able to transfer, or spend, substantial amounts without using the formal financial system (De Koker, 2003:91).

2.3.1 Underground banking

"Underground banking" is a generic term used to describe any informal banking arrangement, which runs parallel to, but generally independent of, the formal banking system (McCusker, 2005:1). Underground banking systems are also referred to as "alternative remittance systems" by the Financial Action Task Force (FATF), "informal funds

transfer systems" (World Bank & International Monetary Fund), and "informal value transfer systems (IVTS)" by the (US Financial Crimes Enforcement Network – FINCEN) (McCusker, 2005:1).

Maimbo (2003:8) found that underground banking is used for moving proceeds of crime and money laundering. Underground banking appears in various forms: some schemes involve bulk cash and currency smuggling and other more complex schemes involve the transfer of value of currency, without necessarily relocating the money (McCusker, 2005:1). A more detailed explanation of these underground banking structures is provided below.

2.3.1.1 Currency smuggling: An underground banking technique

Initially laundering money required a physical effort (Bortner, 1996:1). The art of concealing the existence and the illegal application of income, and then disguising that income to make it appear legitimate required that the launderer have the means to physically transport the hard cash (Bortner, 1996:1). These methods ranged from flying cash out of the country and depositing it into a foreign bank account with less stringent laws, to the classic approach of a "smurf", which was to deposit cash at the bank (Bortner, 1996:1).

"Smurfing" is banking industry jargon used to describe the act of splitting a large financial transaction into smaller transactions to avoid scrutiny by regulators or law enforcement. It is commonly used in the context of money laundering and has been known to appear in official Federal criminal indictments (Wikipedia, 2007:1). The term is synonymous with "structuring a deposit" and it originates from an image of many identical, small transactions. Those cash couriers that smuggle the cash are known as "smurfs" in this context (Wikipedia, 2007:1).

Bortner (1996:1) states that this type of currency smuggle occurred in the United States when the US Bank Secrecy Act (BSA) became

effective and platoons of cash couriers assaulted lobbies of banks with thousands of cash deposits of just under US$ 10,000. The idea was to structure the cash deposit at just under US$ 10,000, to keep the transactions from being detected for reporting purposes to the regulators.

Today, the conveying of currency across borders has been demonstrated to be one of the primary methods of currency smuggling and money laundering and, as such, member countries of the Egmont Group have been asked to consider setting up mechanisms for monitoring cross-border currency movements (Roper, 2001:96).

In light of the trend of cross-border money laundering, South Africa is now a member country of the Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG) and the Egmont group of Financial Intelligence Units (FIUs), and is reviewed yearly by FATF, in order to measure the country's compliance with international AML and counter terrorist financing (CTF) regulations (Michell, 2005:18). South Africa has also drafted and implemented legislation that seeks to counter money laundering and classic currency smuggling techniques as described above.

Section 4 of the Prevention of Organised Crime Act 121 of 1998 stipulates that when a criminal conceals proceeds of criminal activity, whether in a bank account or any other place, then this can be classified as the crime of money laundering.

In this context, the term "proceeds of crime" means the cash (currency) that is concealed and smuggled. "Proceeds of crime", in a broader context, also means "any property or any service, advantage, benefit, or reward which was derived, received, or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act [Prevention of Organised Crime Act], in connection with or as a result of any unlawful activity carried on by any

person, and includes any property representing property so derived" (POCA Act, 1998:2).

Elements of the money laundering crime are identifiable in three main stages: placement of dirty money (proceeds of crime), layering of dirty money, and integration of dirty money (Goredema, 2003:184).

To obtain a more detailed explanation of the elements and to consider the patterns of money laundering within southern Africa, one needs to view money laundering in its various dimensions.

Currency can be smuggled and laundered through various channels and, according to Goredema (2003:184), three dimensions are evident, which are:

- **Internal money laundering**, which can be characterised by the laundering of proceeds of, or assets derived from, crime within the country where the crime was committed;
- **Incoming money laundering**, in which the proceeds or assets laundered are derived from crimes committed outside the country and thereafter introduced into the country; and
- **Outgoing money laundering**, in which the proceeds of crimes committed within the country are laundered through exportation (to one or more countries).

Placement can occur in any of the three varieties of laundering (Goredema, 2003:184). So can layering and integration of the laundered assets. It is clear that, in the case of internal laundering, all three phases would occur in the same jurisdiction (Goredema, 2003:184). Where laundering is incoming, the money may have been kept out of the formal banking institutions until its introduction into the jurisdiction in which placement is to occur (Goredema, 2003:184). The same goes for outgoing laundering (Goredema, 2003:184).

Subsequent to acquisition of the proceeds of crime, the launderer may conceal them, with a view to smuggling the currency to a foreign jurisdiction (Goredema, 2003:184). The concealment *per se* of proceeds of crime (currency) constitutes laundering, even though it precedes placement in any financial (banking system) or commercial system (Goredema, 2003:184).

An example of such an underground banking technique involving currency smuggling in South Africa is recorded in the case of *Mohamed Suliman Vaid and Moshena Vaid versus the National Director of Public Prosecutions (*2001). In *Mohamed Suliman Vaid and Moshena Vaid versus the National Director of Public Prosecutions (*2001), two currency smugglers attempted to smuggle US $ 130,000.00 (R910,000.00) across the South African-Swaziland border post. Mr Suliman had US $ 40,000.00 concealed and stashed down his underpants, his wife, Mrs Suliman, had US $ 90,000.00 concealed in pockets of a specially designed bodysuit that she wore under the long black hijab that covered her whole body and only had an opening that revealed her eyes. Upon closer investigation, police investigators made some discoveries that caused them considerably more concern. Before getting caught, Mr Vaid had travelled from his home in Durban South Africa through Swaziland to neighbouring Mozambique 150 times in 18 months. The South African police indicated that there was some connection between the incident and Dubai.

The *modus operandi* of the accused in the above-mentioned case seems to be similar to that of the case involving a recent High Court currency seizure and forfeiture matter in *Abdul Jabbar versus the National Director of Public Prosecutions* (2003), which is further discussed below. The accused would travel frequently between countries within one month; he seemed to have no formal business interest; had a link to a tax haven such as Dubai; and were caught with a large sum of US dollars in his possession.

A typical currency smuggling scheme will include the use of three to ten and even more people to physically transport the currency from point A to point B. In *Abdul Jabbar versus the National Director of Public Prosecutions (2003),* a Pakistani national attempted to smuggle US $ 345,782.00 in cash out of the country. The suspect was on his way to Dubai when the National Prosecuting Authority's Directorate of Special Operations (Scorpions) arrested him at Johannesburg International Airport.

The Scorpions searched Mr Jabbar and found US $ 345,782.00 (R 2,420,474.00 million) wrapped in foil and hidden in a metal cooking pot, which the suspect carried in his hands through customs (Chinner, 2004:12). The High Court documents also revealed that Mr Jabbar frequently travelled between Dubai and South Africa monthly, and had smuggled approximately R 20 million over a few months to Dubai. The cash was forfeited to the state's Criminal Assets Recovery Account (CARA).

The court papers in *Abdul Jabbar versus the National Director of Public Prosecutions (2003)* also revealed that the United Arab Emirates, and in particular Dubai, was continually used as a receiving or conduit country for smuggled currency, with special reference to United States dollars. Adding to that, previously there are countries that were blacklisted by the FATF for not combating money laundering and currency smuggling. These countries are known as Non-cooperative Countries and Territories (NCCT) (Michell, 2005:27). The FATF listed 23 countries around the world as non-cooperative countries during a 2004/2005 review (Michell, 2005:27).

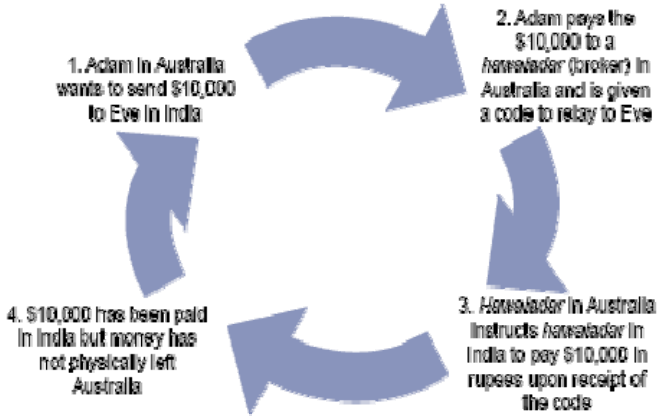
Many other organised crime groups that handle bulk cash need to move their illegal profits from place to place and even from country to country. For example, armed robberies of cash-in-transit in the sub-region are committed in South Africa by relatively well-trained groups

that have access to weaponry, including automatic fire arms (Goredema, 2003:188). Between 1996 and 1998, armed robbers seized more than R 150 million (US$ 15 million) in 854 violent cash-in-transit attacks (Goredema, 2003:188). At the end of June 2002, two ”busts”, in the Douglasdale suburb, north of Johannesburg, and in Roodepoort, on the West Rand, yielded massive seizures of drugs and the haul was valued at R 2.7 billion (US$ 270 million) (Goredema, 2003:186). Large criminal organisations planning and executing crimes of this magnitude will definitely have an organised way of moving their proceeds of crime, and bulk cash, as mentioned above, is definitely smuggled from one point to another using a similar currency-smuggling method to those mentioned above.

2.3.1.2 Hawala schemes: An underground banking technique

Hawala is another underground banking system (McCusker, 2005:1). The hawala system is vulnerable to abuse by money launderers and those seeking to finance terrorism (Maimbo, 2003:8). Whatever term is used across the world, the basic principle of hawala remains the same, and it involves the transfer of value of currency, without necessarily relocating the money (McCusker, 2005:1). A typical hawala currency transfer procedure serves to illustrate the basic process shown in Figure 2.1 below.

Figure 2.1: Hawala process



Source: McCusker (2005:2)

In this way, value may be transferred to and from both jurisdictions. In either case, the hawaladars need to be paid for their service. For example: if a hawaladar has concluded a hawala transaction from Pakistan to South Africa and the money is paid out to a recipient in South Africa, then the hawaladar in South Africa also needs to be paid a fee for the service in South Africa (McCusker, 2005:1).

Underground banking transactions in the hawala system require no identification from either the remitter or receiver of the funds save for the exchange (via telephone, fax or similar) of a simple password between remitter and recipient of the funds (McCusker, 2005:2). This so called “anonymity” with regard to sending and receiving transactions is a major breach of basic money laundering legislation. The absence of customer identification, financial transaction records and business documentation could make the use of the hawala system attractive for laundering the proceeds of criminal activity (Maimbo, 2003:9).

On the other hand, some more detailed research had been done by Harjit Singh Sandhu from the International Police Organisation (INTERPOL) and Patrick M. Jost, from FINCEN, where they explain the way in which hawala is used to facilitate money laundering (Jost & Sandhu, 2000:1). Their research is described in the section below.

2.3.1.2.1 The origins of hawala underground banking

Cited below, Jost and Sandhu (2000:7) describe the origins of hawala underground banking. They go further and explain the Arabic and Middle Eastern coded accounting numerical and techniques utilised by hawala underground bankers (Jost & Sandhu, 2000:7). The Arabic and Middle Eastern writing and numerical is cited in this research report as part of the research, in order to present the phenomena associated with and dynamics of the hawala money laundering scheme fully.

According to Jost and Sandhu (2000:7), a hawala operator is a known as "*hawaladar*" (हवालादार). In their research, Jost and Sandhu (2000:1) found that hawala is an alternative or parallel remittance system. It exists and operates outside of, or parallel to, "traditional" banking or financial channels. It was developed in India, before the introduction of western banking practices. Their research also confirmed that hawala has no paper trail, with regard to the real identity of the person that is sending or receiving the money (Jost & Sandhu, 2000:3).

The Arabic root s-r-f (ص ر ف) has, among other meanings, "pay" and "disburse". The Arabic word for "bank", *masrif* (مصرف), comes from this root. It is also the basis for the Farsi words *saraf* (صراف), which means a "money changer" or "money remitter" (hawala dealer) and *sarafi* (صرافی) which is the name for the business (Jost & Sandhu, 2000:7). The authors found that hawala predates 'traditional' or 'western' banking (formal banking); the first 'western bank' in India was the Bank of Hindustan, established in Calcutta around 1770 (Jost & Sandhu, 2000:7).

Jost and Sandhu's (2000) research brings more detail to the vague approach of McCusker's (2005) research. Contrary to a lot of claims that the hawala system is paperless and that there is no record of subjects who send money, Jost and Sandhu found that, in fact, there is a paper trail (Jost & Sandhu, 2000:8). However, this paper trail is mostly in the form of codes and coded accounting, which is discussed below.

2.3.1.2.2 Hawala paper trail and "coded accounting"

Jost and Sandhu (2000:8) found that the hawaladar does have a form of "coded bookkeeping", and start off by explaining the relevant codes in numerals as indicated in Table 2.2 below. Hawala bookkeeping emphasises keeping track of how much money is owed to whom (Jost

& Sandhu, 2000:6). Charts are usually handwritten, and it is not uncommon for English and another language to be used.

Numerals: for reference, here are the forms of the numerals as written in Hindi, Gujarati, Punjabi, Bengali, Urdu, Arabic and Persian (Farsi/Dari) (Jost & Sandhu, 2000:8).

Table 2.2: Middle Eastern and Asian numerals reference table

	1	2	3	4	5	6	7	8	9	0
Hindi	१	२	३	४	५	६	७	८	९	०
Gujarati	૧	૨	૩	૪	૫	૬	૭	૮	૯	૦
Punjabi	੧	੨	੩	੪	੫	੬	੭	੮	੯	੦
Bengali	১	২	৩	৪	৫	৬	৭	৮	৯	০
Urdu	١	٢	٣	۴	۵	۶	۷	٨	٩	٠
Arabic	١	٢	٣	٤	٥	٦	٧	٨	٩	٠
Persian	١	٢	٣	۴	۵	۶	٧	٨	٩	٠

Source: Jost and Sandhu (2000:8)

The coded accounting tables displayed in Jost and Sandhu's research paper can be used as a guide table during investigations. The authors further supported their work by providing actual extracts of investigative records from INTERPOL and FINCEN (Jost & Sandhu, 2000:6).

Below in Table 2.3 is a sample chart that is based on records analysed by Jost and Sandhu during a recent investigation, and is representative of the records that might be encountered during a hawala investigation (Jost & Sandhu, 2000:6).

Table 2.3 Sample chart: Hawala records

98	Vinod	100000	37.6	2659.57	F-1202
16/6/98	Ashish	250000	39.25	6369.42	F-1203
16/6/98	Nitin Bhai	350000	42.3	8274.23	B-8146
17/6/98	DK	50000	38.75	1290.32	F-1204
17/6/98	Suresh Kumar	300000	39.25	7643.31	B-8147
17/6/98	Anil	200000	40.1	4987.53	S-5428
17/6/98	Vinod	150000	39.75	3773.58	F-1205
18/6/98	Manoj	300000	41.25	7272.72	B-8148
18/6/98	Vinod Bhai	350000	42.2	8293.83	L-2160
18/6/98	Ganesh Trading	200000	38	5263.15	५२ त
19/6/98	Suresh Kumar	175000	39.5	4430.37	B-8149

Source: Jost and Sandhu (2000:6)

Hawala bookkeeping emphasises keeping track of how much money is owed to whom (Jost & Sandhu, 2000:6). In light of that and with reference to the sample chart, the first column of the chart indicates the date of the transaction. The second column shows the name of the hawala broker to whom the debt is owed; it is very common to use partial names (e.g. “Vinod”) or codes (e.g. “DK”). The third column presents the amount of the debt. This chart reflects a tendency to do business in multiples of 100,000; so it would not be uncommon to see things like “1.5” for 150,000. The third column indicates the dollar/rupee exchange rate in effect for the transaction. The fourth column shows the value of the transaction in dollars. The fifth column reflects the way in which the payment was made. Notations, such as “F-1202”, usually represent a bank (“F” might be “First Bank”; “B” and “L” would represent other banks) and the check number. The notation ५२ त is for Ganesh Trading, “52 t”, in Hindi language (Jost & Sandhu, 2000:6).

Jost and Sandhu’s work was further supported by a World Bank research paper compiled by Maimbo (2003). The World Bank’s research paper was written after three field visits by Maimbo to Afganistan – two in 2002 and one in 2003. Maimbo confirmed that the

hawala dealers do in fact keep some records (Maimbo, 2003:4). Record keeping is necessary because the hawala dealers obviously need to know how much must be paid out and how much money was taken from the sender. On the other hand, Maimbo's (2003) research does not go into detail about "coded accounting" and "hawala bookkeeping", as does the Jost and Sandhu study.

Maimbo's research has brought greater clarity about the concept of hawala and actually explains its form and structure to a certain extent, based on real field visits and interviews in Afghanistan. In essence, Maimbo found that the hawala transfer system can be abused for money laundering transactions and that the system is vulnerable to abuse by money launderers and those seeking to finance terrorism (Maimbo, 2003:8).

According to Maimbo (2003:8), laundering money through the formal financial system leaves a paper trail, making it vulnerable to detection by law enforcement agencies during an investigation. Hawaladars minimise detection by limiting external access to or oversight of their records and coded accounting records. This absence of business documents could therefore make the use of the hawala system attractive for laundering the proceeds of criminal activity (Maimbo, 2003:9).

2.3.1.3 Legislation relevant to various underground banking schemes

Most underground banking schemes relate to financial crime offences which are covered in the Currency and Exchanges Act 9 of 1933 (South Africa, 1933), the Financial Intelligence Centre Act 38 of 2001 (South Africa, 2001), and the Prevention of Organised Crime Act (POCA) 121 of 1998 (South Africa, 1998), which are discussed below.

Prevention of Organised Crime Act 121 of 1998 (sections 4 & 8)

According to POCA (1998:6), money laundering is defined in section 4 of the Act and reads as follows:

"Any person who knows or ought to have known that property (money) is or forms part of the proceeds of unlawful activities and-

(a) enters into an agreement or engages into any arrangement or transaction with anyone in connection with that property, whether such agreement, arrangement or transaction is legally enforceable or not,

or

(b) performs any other act in connection with such property, whether it is performed independently or in concert with other persons, which has or is likely to have the effect-

(i) of concealing or disguising the nature, source, location, disposition or movement of the said property or its ownership or any interest which anyone may have in respect thereof; or

(ii) of enabling or assisting any person who has committed or commits an offence whether in the Republic or elsewhere-

(aa) to avoid prosecution; or

(bb) to remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence."

This means that, if any person is concealing or disguising the nature, source, location, disposition or movement of cash (currency), which is the proceeds of crime, they are making themselves guilty of money laundering, in terms of section 4 of the Prevention of Organised Crime Act.

Section 8 of the Prevention of Organised Crime Act 121 of 1998 stipulates that any person who is convicted of money laundering can be sentenced to a maximum fine of R 100 million or to imprisonment for a maximum period of 30 years (South Africa, 1998:5).

The Currency and Exchanges Act 9 of 1933 (sections 9 & 3)

The state president has, in terms of section 9 of the Currency and Exchanges Act 9 of 1933, proclaimed exchange control regulations which place certain restrictions regarding the dealing in currency.

Regulation 3 (1) states that:

"Subject to any exemption which may be granted by the Treasury or a person authorized by the Treasury, *no person shall, without permission granted by the Treasury or a person authorized by the Treasury* and in accordance with such conditions as the Treasury or such authorized person may impose –

(a) take or send out of the Republic any bank notes (currency), gold, securities or foreign currency, or transfer any securities from the Republic elsewhere; or

(b) send, consign or deliver any bank notes (currency), gold, securities, or foreign currency to any person for the purpose of taking, sending or removing such bank notes, gold, securities or foreign currency out of the Republic; or

(b) *bis* take any South African bank notes into the Republic or send or consign any such notes to the Republic."

Regulation 3 (3) also states that:

"Every person who is about to leave the Republic and every person in any port or other place recognized as a place of departure from the Republic, who is requested to do so by the appropriate officer shall –

(a) declare whether or not he has with him any bank notes, gold, securities, or foreign currency; and

(b) produce any bank notes, gold, securities or foreign currency which he has with him."

The Financial Intelligence Centre Act 38 of 2001 (section 54)

Section 54 of the above-mentioned act states that cash which is transported or is about to be transported across the borders of South

Africa must be reported before leaving the county to the relevant authorities. The Financial Intelligence Centre Act also makes provision for the seizure and forfeiture of the smuggled currency. It must be added that Chapter 5 and Chapter 6 of the Prevention of Organised Crime Act 121 of 1998 also make provision for the seizure of such smuggled currency.

From the above quotes it is clear that the Prevention of Organised Crime Act 121 of 1998, the Currency Exchanges Act 9 of 1933 and the Financial Intelligence Centre Act 38 of 2001 make the smuggling of currency and money laundering-related schemes a criminal offence.

The convergence from underground banking-related money laundering schemes to integration into the formal banking system will be discussed further below.

2.3.2 Formal banking

All banks in South Africa are regulated by the South African Reserve Bank (SARB) and are administered under the Banks Act 94 of 1990 (South Africa, 1990). Banks are also regulated by the Financial Intelligence Centre of South Africa, under the Financial Intelligence Centre Act 38 of 2001. The Financial Intelligence Centre ("the FIC") was established as South Africa's financial intelligence unit in February 2002, when the Financial Intelligence Centre Act, Act 38 of 2001 was promulgated (Michell, 2006:5).

Parliament passed the Act after extensive engagement of the need to protect the Republic of South Africa's democratic Constitution and the rights afforded to all its citizens and its institutions from the activities of criminals and criminal syndicates (Michell, 2006:5). The Act sought to ensure the sound health of the country's financial system by preventing it from being contaminated and undermined by flows of "dirty" money derived from proceeds of crime (Michell, 2006:5).

There are approximately 33 registered South African banks, and they can be divided into the categories of: Retail Bank, Corporate Bank, Private Bank and Investment Bank. The most well-known South African banks are ABSA Bank Ltd, First National Bank Ltd, Nedbank Ltd, and Standard Bank Ltd. Foreign banks are active in South Africa and are also administered under the Banks Act 94 of 1990. American banks active in South Africa must also comply with United States' (US) laws such as the Office of Foreign Assets Control (OFAC) regulations (31 C.F.R Chapter V). Fox (2005b:17) states that banks with US offices or branches must comply with OFAC regulations.

Fox (2005b:7) writes that one of the OFAC regulations states that a US bank may not transfer or hold funds for an entity when the OFAC has designated the entity as "specially designated terrorist", "specially designate global terrorist", or "foreign terrorist organisations". A US bank must comply with this OFAC regulation, even if the bank is active outside the United States, in this case in South Africa.

2.3.2.1 Formal banking and the Financial Intelligence Centre of South Africa

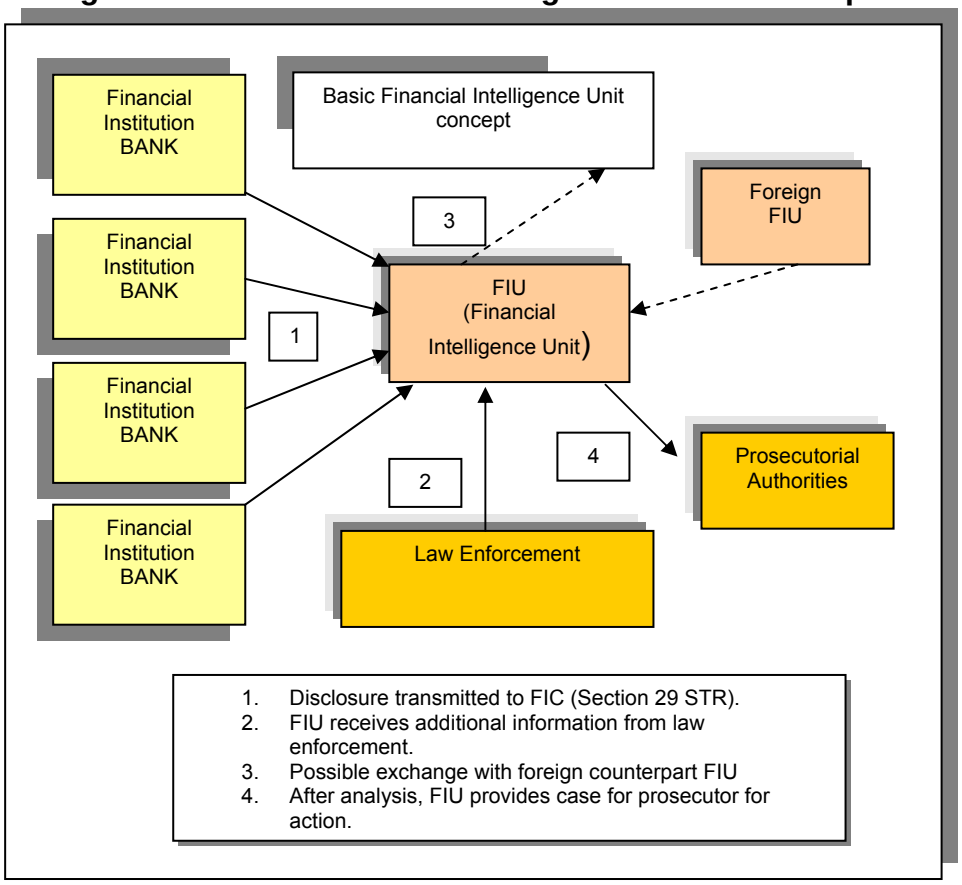
The Financial Intelligence Centre ("the FIC") was established as South Africa's financial intelligence unit in February 2002, when the Financial Intelligence Centre Act, Act 38 of 2001 was promulgated (Michell, 2006:5). The Financial Intelligence Centre (FIC) of South Africa has the responsibility for providing leadership in the implementation of the Republic of South Africa's anti money laundering and combating of financing of terrorism ("AML/CFT") environment (Michell, 2006:6).

On an international level, the FIC also forms part of the Egmont Group of Financial Intelligence Centres (FICs), which comprises 104 countries (Michell, 2006:29). The main purpose of the Egmont Group is to facilitate and enable the sharing of information between FICs across the world (Michell, 2006:5).

South Africa also forms part of the Eastern and Southern African-Money Laundering Group (ESAAMLG), which is a FATF-style regional body and was established in 1999 (Michell, 2006:28). It consists of 14 member countries in the region: the republics of Botswana, Kenya, Malawi, Mozambique, Mauritius, Namibia, South Africa, Seychelles, Tanzania, Uganda, Zambia, and Zimbabwe and the kingdoms of Lesotho and Swaziland (Michell, 2006:28).

Banks must report suspicious transactions, money laundering transactions and terrorist financing transactions to the South African FIC in terms of Act 38 of 2001 (FICA), section 29 – Suspicious Transaction Report (STR) (also known as suspicious activity reports (SARs) in the banking environment in other parts of the world). Figure 2.2 below concisely sums up the Financial Intelligence Centre concept.

Figure 2.2: The Financial Intelligence Centre concept



Source: Financial Intelligence Centre of SA (2004:4)

Also, in South Africa, the provisions to combat the financing of terror (CFT) are incorporated in the Protection of the Constitution and Democracy and Terrorism and Related Act 33 of 2004 (POCDATARA Act, 2004), which was implemented from 20 May 2005 (Michell, 2006:5).

It is a criminal offence when a banker identifies a suspicious transaction and does not report it to the FIC, and any banker that fails to report such a transaction can be imprisoned for a maximum period of 15 years or can have a maximum fine of R 10 million imposed on them in terms of section 68 of the Financial Intelligence Centre Act 38 of 2001.

2.3.2.2 Formal banking and section 29 – Suspicious Transaction Report of the Financial Intelligence Centre Act 38 of 2001

Banks must report all suspicious transactions to the FIC in terms of section 29 of the FIC Act 38 of 2001. The FIC will collect, retain, compile, and analyse all information disclosed to it and obtained by it in terms of the FIC Act. It will not investigate criminal activity, but will provide information to advise and cooperate with intelligence services, investigating authorities and the SARS, which institutions should carry out such investigations (section 44).

Section 29 of the Financial Intelligence Centre Act 38 of 2001 reads as follows:

(1) "A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or suspects that-

(a) the business has received or is about to receive the proceeds of unlawful activities;

(b) a transaction or series of transactions to which the business is party-

(i) facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities;

(ii) has no apparent business or lawful purpose;

(iii) is conducted for the purpose of avoiding giving rise to a reporting duty under this Act; or

(iv) may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed for the South African Revenue Service; or

(c) the business has been used or is about to be used in any way for money laundering purposes;

must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series."

(2) "A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or suspects that a transaction or a series of transactions about which enquiries are made, may, if that transaction or a series of transactions had been concluded, have caused any of the consequences referred to in subsection (1) (a), (b) or (c), must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions."

(3) "No person who made or must make a report in terms of this section may disclose that fact or any information regarding the contents of any such report to any other person, including the person in respect of whom the report is or must be made, otherwise than-

(a) within the scope of the powers and duties of that person in terms of any legislation;
(b) for the purpose of carrying out the provisions of this Act;
(c) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
(d) in terms of an order of court."

(4) "No person who knows or suspects that a report has been or is to be made in terms of this section may disclose that knowledge or suspicion or any information regarding the contents or suspected contents of any such report to any other person, including the person in respect of whom the report is or is to be made, other wise than-
(a) within the scope of the powers and duties of that person in terms of any legislation;
(b) for the purpose of carrying out the provisions of this Act;
(c) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
(d) in terms of an order of court."

2.4 SUMMARY

In summary, underground banking has long been regarded as a conduit for money laundering by criminal organisations and arguably by terrorist networks (McCusker, 2005:1).

The organised structures within underground banking are vulnerable to abuse by money launderers and those seeking to finance terrorism (Maimbo, 2003:8). The formal banking systems are also vulnerable to abuse by money launderers (Maimbo, 2003:8). Money laundering is an existing problem and research figures indicate that a total of US $ 22 billion was laundered through the financial systems of Southern Africa in 1998 (Goredema, 2003:206).

Early in this century South Africa designed appropriate legislation to address this problem and made funds available for the establishment of the Financial Intelligence Centre. The Financial Intelligence Centre (FIC) of South Africa has the responsibility of providing leadership in the implementation of the Republic of South Africa's anti money laundering and combating of financing of terrorism ("AML/CFT") environment (Michell, 2006:6).

Clearly, proceeds of crime transactions, terrorist financing, and money laundering transactions are very difficult to detect. However, banks can be fined millions and bankers can face jail sentences if they fail to put measures in place to detect and report suspicious transactions, proceeds of crime transactions, and money laundering transactions.

Chapter 3, which follows, looks at what type of advanced accounting software is available for detecting and investigating suspicious transactions, proceeds of crime, and money laundering transactions that enter the formal banking systems.

CHAPTER 3:
ADVANCED ACCOUNTING SOFTWARE SYSTEMS

3.1 INTRODUCTION

Banks have an enormous task to comply with legislation and to identify proceeds of crime, money laundering transactions, and terrorist financing transactions that flow through banking systems. On the other hand, law enforcement agencies face an even bigger challenge in prosecuting money launderers and terrorist financiers.

Previously, several banks have failed to properly investigate the flow of incoming and outgoing money from their banking systems and have been fined millions. Most of these banks could have prevented these very big fines if they had utilised advanced accounting software, automated transaction filters and very effective Anti Money Laundering Systems (AML Systems), which scan financial transactions and high-risk customer names automatically. A good example of this is when Riggs Bank was fined US $ 25 million (R 162 million) in 2004, for failing to identify and report suspicious transactions (Fox, 2004:1). Arab Bank PLC was fined US $ 24 million (R 156 million), for similar AML failures (Fox, 2005a:3), and ABN AMRO Bank was fined US $ 80 million (R 520 million) in December 2005, for gross AML failures (Fox, 2005b:7).

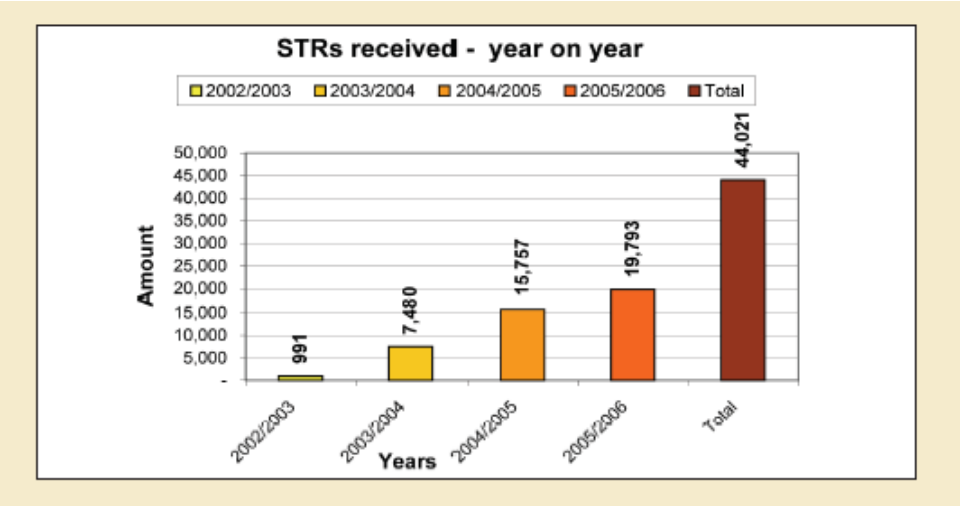
In light of the above, it makes sense for banks to avoid these large fines by implementing a comprehensive AML compliance policy, with a vigorous transaction investigation and monitoring approach at the core of the AML policy. Some advanced accounting software and AML systems which can be used to detect proceeds of crime and money laundering transactions are discussed below.

3.2 ADVANCED ACCOUNTING SOFTWARE FOR INVESTIGATIONS

Michell (2006:11) has indicated a sharp rise in South African banks making suspicious transaction reports (STRs). Figure 3.1 below indicates the systematic rise in suspicious activity reports (SARs) that have been made. Towards the end of the 2005 financial year, there was a significant increase in the reports received by the Financial Intelligence Centre (FIC); the number of reports received increased by 186% from 8,471 (in 2003/4) to 24,228 (in 2004/5) (Michell, 2006:11).

Figure 3.1

Suspicious Transaction Reports received by the Financial Intelligence Centre of South Africa, 2002 – 2006



Source: Michell (2006:16)

Michell (2006:16) states that the FIC has received 44,021 STRs in the past five years, from 2002 to 2006.

This might be an indication that money laundering is on the rise in South Africa; on the other hand, it might indicate that money laundering is now more exposed than before.

Whatever conclusion one wants to draw from the statistics supplied by the South African FIC, some questions arise, such as: what is being done about this; are the police investigating this alleged money laundering; and what investigative tools, such as computers and accounting software are used to trace and investigate money laundering?

There are several advanced accounting software, transactions analysis, and AML systems available, which can be used as investigative tools during a forensic investigation involving the proceeds of crime and money laundering transactions.

3.2.1 Types of advanced accounting software

Some of the world's leading financial services brands have begun taking AML very seriously. American Express, United Bank of Switzerland (UBS), Wells Fargo Bank and Barclays Bank are just some of the leading global banks that have already made significant investment in mitigating the reputational risk from money laundering (Searchspace Ltd, 2004a:3). Table 3.1 provides a breakdown of the different types of investigative systems which can be used to detect possible proceeds of crime and money laundering transactions.

Table 3.1: **Types of Anti Money Laundering Systems**

AML SYSTEMS (Anti Money laundering Systems)				
AML System design description	**AML System name**			
Information Provider	Complinet	World-Check	Factiva	Thompson
Simple Filters	Logica CMG'S	Hotscan	Thompson	
Advanced Filters	Fircosoft OFAC Agent			
Rules-based Systems	AmericaSoft	STP Detector	Neteconomy	
Scenario Spotters	Data4S Pinpoint	Mantas	ACI	
Customer Modellers	Searchspace Ltd	FORTENT		

Source: Searchspace Ltd (2004a:14-26)

Since the events of 11 September 2001, when terrorists hi-jacked planes and flew them into key buildings in the US, such as the World

Trade Centre and the Pentagon, new legislation (USA Patriot Act, Title III) to identify money laundering and terrorist financing transactions have been implemented in the US (Searchspace Ltd, 2002:1).

After 11 September 2001, South Africa also acted swiftly, and the provisions to combat the financing of terrorism and money laundering in South Africa were incorporated into the Financial Intelligence Centre Act 38 of 2001, and the Protection of the Constitution and Democracy and Terrorism and Related Activities Act 33 of 2004 (POCDATARA), which was implemented from May 2005 (Michell, 2005:5). This Act places the onus on bankers in South Africa to report suspected terrorist financing transactions to the FIC of South Africa. The legislation relevant for combating financial crime in its various dimensions is discussed in more detail in Chapter 2 of this research report.

To comply with these new Acts, a much more sophisticated approach to investigating dirty money flowing through the banking system is required. The demand for AML software systems had been rising in recent years, fuelled by recent money laundering scandals, but the 11 September 2001 terrorist attacks brought a niche industry to the market (Searchspace Ltd, 2002:1).

Although the use of advanced algorithms to catch criminals may sound far-fetched, financial institutions face little alternative since they lack the manpower to analyse millions of transactions, any of which could be a money laundering transaction (Searchspace Ltd, 2002:1).

3.2.1.1 Anti Money Laundering information providers

World-Check, Complinet and several other web-based software companies exist that specialise in keeping track of and maintaining up-to-date databases of government or United Nations sanctions lists of terrorists, criminals and regional crime trends in countries.

In particular, these software companies maintain databases on Politically Exposed Persons (PEPs), which is a major threat for banks and their reputation. An example of a massive PEP failure is when a Swiss Bank was ordered in 1997, by Switzerland's highest court, to release and hand over more than US $ 500 million that was stashed away in this Swiss Bank by the former political president of the Philippines, Ferdinand Marcos (Leppan, 2005:2).

The Complinet Client Screening 2006 Enterprise Edition software allows a bank to access and run sophisticated name-matching algorithms that will run automated screens for matches with PEPs that might be already embedded in the bank's system or might be a new client (Complinet, 2006:7).

3.2.1.2 Simple filters

Simple filters check individual payment transactions against lists of known high-risk individuals. Unfortunately, the drawback of this system is that it will not detect unusual or suspicious behaviour; it simply conducts automated filtering of names (Searchspace Ltd, 2004a:16). Typical simple filters do not include facilities to support the investigations' process; examples are Logica CMG's Hotscan and Thompson (Searchspace Ltd, 2004a:16).

3.2.1.3 Advanced filters

Advanced filters check individual payment transactions against government lists of known individuals and organisations; for example, organisations that are considered to be engaged in terrorist activities (Searchspace Ltd, 2004a:16).

Advanced filters also often include the facility to write simple rules that can be applied to the individual transaction. For example, a payment from the US to Iran of US $ 50 000 can be automatically identified and blocked because Iran is a country under sanctions by the US.

A system of this type can be embedded into the authorisation path of a bank's payment system, to block the payments to and from individuals on embargo lists.

On the other hand, the drawback of this system is that such a system alone will not help a bank to detect and investigate money laundering. An example of such an advanced filter is FircoSoft OFAC Agent (Searchspace Ltd, 2004a:16).

3.2.1.4 Rules-based system

With the rules-based system, or so called "expert systems", the bank can write a rule that will produce an alert, for example a Cash Threshold Report (CTR), when a bank-specified threshold is exceeded. An example of such a rule might be: "is a transaction a cash transaction and is it more than R 10 000?" This might be a reportable transaction to the FIC of South Africa. So, this system automatically identifies the reportable transaction. This system can also write more "advanced" rules such as: "has the customer signed more than ten cheques this month?" This system also introduces the concept of profiles. A profile is a representation of what is expected behaviour for a certain category or segment of customers (Searchspace Ltd, 2004a:17).

One of the drawbacks of this type of AML system is that it monitors individual transactions based on a rule, such as going over an amount. However, an effective AML investigative system must be able to monitor a suspect's whole banking profile and all the different accounts and not only an individual transaction without context. The second drawback of this type of investigative system is that the rules-based system requires a team of experts to write and maintain all the rules and profiles. This can be very complex and costly in terms of running cost (Searchspace Ltd, 2004a:18).

3.2.1.5 Scenario spotters

An example of this type of AML system is MANTAS. This scenario spotter monitors customer activity for well-known high-risk scenarios. This advanced AML system augments the rules and simple profiles typically found in rules-based systems with data-mining techniques, such as peer analysis, outlier detection, sequence matching, neural networks and link analysis (Searchspace Ltd, 2004a:19). The alerts produced by scenario spotters are of very high quality compared to rules-based systems. Scenario spotters typically include a library of scenarios of well-known high-risk money laundering cases (Searchspace Ltd, 2004a:19).

As with rules-based systems, the bank will need to write new money laundering scenarios and also require access to a history of base transaction data, to run its pattern detection algorithms; a scenario spotter must keep records of the history of all the base transactions in its database (Searchspace Ltd, 2004a:19).

3.2.1.6 Customer modellers

Enterprise-wide risk systems that monitor all customers' current activity against a model of how that individual customer normally uses each product are known as "customer modellers". Instead of data-mining transactions for well-known money laundering patterns, a customer modeller makes an automated risk assessment and ranks all customers according to the degree of suspicion of money laundering, before presenting the highest-risk cases to the financial institution investigations' team for further human investigation (Searchspace Ltd, 2004a:21).

The automated risk assessment process is used to conduct many independent investigations in parallel on each customer. Each investigation may use a different detection approach, such as outlier detection, peer comparison or link analysis, to produce evidence. The bank-defined risk weightings and the overall value of the transactions

affect the systems' overall risk assessment of each customer (Searchspace Ltd, 2004a:21).

An investigation approach that is based on the collection of evidence means that all customer activity can be ranked according to risk (Searchspace Ltd, 2004a:21). Ranking all customer activity according to risk avoids the drawbacks of the "black or white" decisions made by rules-based systems. It also means that the investigation team can focus its efforts on the highest risks. This approach maximises the effectiveness and minimises the cost of running the investigation process while providing extremely effective protection (Searchspace Ltd, 2004a:22).

For this type of AML investigative system to work effectively, a customer modeller must model how each customer uses the financial institution's products. As a side effect, the system builds a full client view, which is a valuable resource that can also be used to reduce fraud loss and drive increased sales (Searchspace Ltd, 2004a:22). In addition to modelling normal customer behaviour, a good customer modeller should provide a filter and rules interface and expose all of the summaries and profiles to allow the bank to detect well-known money laundering patterns and transactions to and from individuals and organisations on an embargo list (Searchspace Ltd, 2004a:22). An example of such as an AML system is Searchspace Ltd (now re-branded as FORTENT) (Searchspace Ltd, 2004a:22). This AML system is an example of a customer modeller that also includes the pattern detection technologies found in the most advanced scenario spotter.

On the other hand, the AML investigative systems discussed above also have shortcomings, and are not always one hundred percent fail proof. What many banks have to still discover is that there is a problem that tends to go unnoticed until it is too late (Marinos, 2005:1). In the crucial gap between these AML investigative strategies and their

execution, there is a quiet crisis in data management that is elevating the same risks as these AML strategies are intended to mitigate (Marinos, 2005:1). This means that a bank can implement these very sophisticated AML investigative systems, but if a teller at branch level types in a wrong spelling of a name, then this will influence the accuracy of the name-matching capacity of the investigative system and cause high-risk customers not to be picked up by the automated name-matching filter of some of these AML systems.

According to Marinos (2005:1), the sobering truth is that ineffective AML strategies, poor data quality, and poor data integration into these advanced accounting and AML investigative systems are often to blame for ineffective AML programmes. By the time the regulators have arrived for a money laundering investigation, or criminal elements have laundered illegal gains, the damage has already been done (Marinos, 2005:1).

According to Marinos (2005:1), this data management issue is a quiet crisis and is happening because, instead of being accorded a priority status as one of the most fundamental components of an AML programme, data quality tends to be treated as a byproduct of business processes, such as account opening, transaction processing and tax reporting. Without effective data management disciplines in place, human and systems' errors, poor control environments, and security flaws begin to take their toll (Marinos, 2005:1).

Another shortcoming of these advanced accounting systems and AML systems is the irrelevant alerts, which are generated automatically by the investigative system; these alerts are known as "False Positives" (Sanjaya, 2005:4). These False Positives are transactions over a set limit that are marked as suspicious, but that do not represent any existing identified risk (such as money laundering) to the bank (Sanjaya, 2005:4).

Securing a mortgage, for example, could represent a transaction that is of an unusually large size for an existing account and will obviously generate an automatic alert by the system; however, this same transaction is also legitimate and does not pose a money laundering risk, because the money entering the account is not the proceeds of crime (Sanjaya, 2005:4).

The problem with these False Positive alerts is that they can easily overwhelm a bank by requiring it to dedicate many resources to the investigation process, while taking the focus off other transactions which might be more representative of a true money laundering risk (Sanjaya, 2005:4).

Therefore, while many AML solutions have been in place for some time within the financial community, the efficiency with which these AML solutions have been able to detect, alert the institution to, and prevent potential money laundering schemes have depended on the quality of the data collected by the financial institution, and the capabilities of the tools that are tasked with analysing the data (Sanjaya, 2005:10).

To the question, what type of advanced accounting software is available to assist in tracing proceeds of crime? The respondents replied as follows:

- There is advanced accounting and AML investigative software available, and the respondents mentioned Excel Accounting, i2 Ltd Analyst Notebook, Searchspace Ltd-Fortent Ltd, or the Mantas Inc system (5/30 respondents);
- A majority of the respondents do not know of any such advanced accounting software and AML investigative systems (25/30 respondents);

- The majority of respondents have never received training in the use of advanced accounting software to trace proceeds of crime into banking systems (25/30 respondents).

To explain the above results, most of the respondents who could contribute relevant and specific technical input about advanced accounting software systems which can be used to investigate the flow of proceeds of crime transactions were from the financial services industry, such as banks.

However, on the basis of the above-mentioned feedback from respondents, it is clear that the respondents have knowledge on the legal aspects of money laundering, but not many AML practitioners from the sample have the required expertise when it comes to using advanced accounting software to investigate the flow of proceeds of crime entering the formal banking system. Also, it is clear that many respondents have not received training in the use of advanced accounting software to investigate the flow of proceeds of crime entering the formal banking system.

This is quite surprising because, according to De Koker (2003:117), the Detective Service of the SAPS has an existing capacity to investigate suspicious transaction reports and money laundering. The Detective Service consists of the Commercial Branch, the Organised Crime Branch, and the Serious and Violent Offences Branch (De Koker, 2003:117). However, De Koker (2003:117) also states that this capacity of the Detective Service of the SAPS will have to be expanded and improved on to enable it to investigate all the reports of suspicious transactions.

De Koker (2003:118) claims that not many resources have been invested in the development of an existing capacity for the SAPS to investigate STRs. However, core staff members at the Head Office of the Commercial Crime Branch have received training in money

laundering control (De Koker, 2003:118). It is not clear whether the training that was provided to the Head Office of the Commercial Crime Branch was focused on the legislative angles of money laundering control, rather than on the financial analytical side. If this were so, this might be a reason for the limited financial analytical insight shown by respondents.

To further compound this problem, it seems as if the Head Office of the Commercial Crime Branch has not provided downward training on the use of advanced accounting software to trace proceeds of crime into banking systems to the Johannesburg Commercial Crime Branch. The topic appeared to be not very clear to respondents from this unit. In fact, the interviews revealed that none of the members of the Johannesburg Commercial Crime Unit, nor the Johannesburg Organised Crime Unit was ever provided with training in the use of advanced accounting software to trace proceeds of crime into banking systems.

It is, therefore, obvious, that, if the respondents received classic legal theories training and no training in technical financial analysis in proceeds of crime and money laundering investigations, this revealed a shortcoming in the SAPS training in money laundering-related typologies, with specific reference to financial analysis during investigation. Respondents from the Johannesburg Commercial Crime Unit and the Johannesburg Organised Crime Unit could not provide the names of automated or non-automated advanced accounting software systems which can be used as an investigative tool during proceeds of crime and money laundering investigations.

On the other hand, the financial services respondents gave very relevant technical feedback, which is discussed further. Below, some respondents specific feedback is cited; the essential aspects of this feedback had to be extracted and concisely stated because some

respondents gave very detailed and technical feedback on these systems.

In some instances, it was necessary for the respondents to provide "screen shots" and descriptions, in order to explain exactly how these advanced accounting functions are used in practical financial investigations. For example, respondent 10, a Chartered Accountant (CA), is specifically cited because the respondent displayed superior insight into these advanced accounting techniques and also provided practical explanations and systems screen shots.

From the responses of the respondents it is clear that there is also non-automated advanced accounting software, which does not have to be embedded in a bank's transaction system. These non-automated advanced accounting software systems can be used by the individual as a forensic investigative/accounting tool to investigate the flow of dirty money and to analyse complex money laundering schemes.

This accounting software can be used on a normal laptop computer and does not need to be connected to a bank's transactions' system for financial analysis, during proceeds of crime or money laundering investigation. This software can be used for reactive money laundering investigations by forensic audit firms and police detectives, instead of the pro-active automated AML systems implemented by banks.

3.2.1.7 Excel-Microsoft

Most accountants and forensic audit firms use Microsoft Excel to conduct financial modelling, prepare financial statements, and conduct financial analysis and forensic accounting (Respondent 10, 2007).

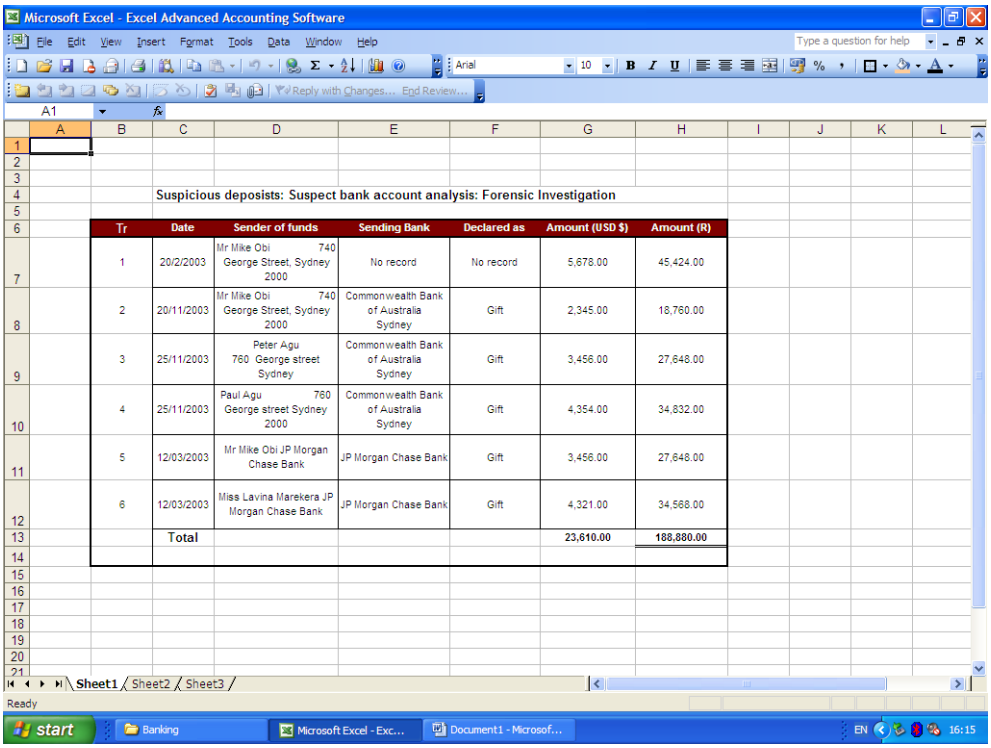
The Excel program has various different financial accounting fields, and many banks and financial companies use this program to store financial data needed to interrogate and analyse their bank's flow of funds (Respondent 10, 2007).

Some functions relevant to tracing proceeds of crime transactions and money laundering transactions are discussed below.

3.2.1.7.1 Excel AutoSum function

AutoSum allows the forensic investigations' specialist to calculate up to 65,536 different financial data entries in a bank account or any other financial record with the click of one button; the advanced accounting program "runs" the figures itself and can calculate the totals of 65,536 rows in a few seconds (Chester, 1994:19). AutoSum function also calculates 256 columns horizontally in a few seconds. Below is a screen shot example of how an Excel financial flow chart can be used in a forensic investigation/forensic accounting analysis of a bank account.

Figure 3.2: Financial flow chart – Excel 2003 – system screen shot



Source: Respondent 10 (2007)

3.2.1.7.2 Excel Data Sort function

This function allows the forensic investigations' specialist to sort financial data of up to 65,536 different entries from smallest amounts to

biggest amounts in a few seconds (Chester, 1994:443), or the forensic investigations' specialist may choose to sort financial data from different depositors, different locations across South Africa, or whatever the analysis scenario requires.

The excel data sort function can be used to sort a bank account's specific activity; for example, it can sort descending or ascending, cheque activity, then credit card activity, and then Internet transfer activity with the data-sorting toolbar (Respondent 10, 2007). This allows the financial investigator to view certain high-risk transactions by specific product.

3.2.1.7.3 Excel Data Auto filter and Advanced Filter function

This function allows the forensic investigations' specialist to filter 65,536 different financial data entries vertically and 256 financial data entries horizontally at the same time in a few seconds (Chester, 1994:443). Up to 65,536 names and surnames of people can also be filtered with this software.

This advanced accounting functionality of Excel is used during investigations by three of the 30 respondents from the sample.

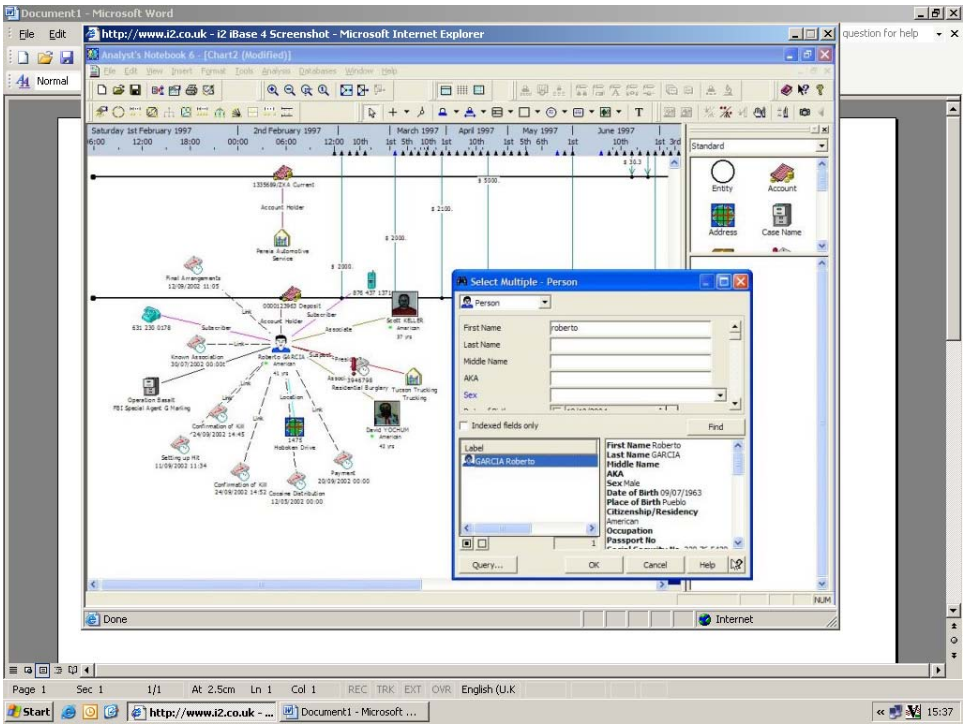
3.2.1.8 i2 Ltd Analyst Notebook

Accurate and focused forensic investigations require the ability to store and retrieve volumes of disparate data gathered as they collect information. i2 Ltd iBase is a sophisticated solution for capturing, controlling and analysing multi-source data in a secure environment (i2 Ltd, 2007:1).

i2 Analyst Notebook has various functions and can assist the forensic investigator with many complex investigations. This investigative system provides the optimum environment for effective link and timeline analysis (i2 Ltd, 2007:1).

The system also allows for the sorting and interrogating of financial transactions into other formats or into chronological order. Figure 3.3 below provides an example of i2 iBase, which can be used to analyse financial data manually or automatically to generate link and time line analysis and automatic charting in complex investigations (i2 Ltd, 2007:1).

Figure 3.3: i2 Ltd IBase 5-Automatic Charting screen shot



Source: i2 Ltd (2007:1)

Specifically designed for analysts and investigators, i2 iBase incorporates a range of powerful functions tailored to their needs. Once the data is captured, a wide range of analytical and query options bring it to life (i2 Ltd, 2007:1).

Analyst Notebook can be used for various investigations and analysis, and, specifically, it can assist in analysing large numbers of telephone numbers, financial transactions, and graphical link charts (Respondent 19, 2007). i2 Analyst Notebook is used during investigations by two of the 30 respondents from the sample.

3.3 SUMMARY

The systematic rise in suspicious activity reporting by banks in South Africa indicates that they take money laundering very seriously. The statistics of the FIC show that, towards the end of the 2005 financial year, there was a significant increase in the reports received by the FIC, it increased by 186% from 8,471 (2003/4) to 24,228 (2004/5) (Michell, 2006:11). According to Michell (2006:16), the FIC received 44,021 STRs in the five years from 2002 to 2006.

The banking sector is, therefore, exposed to a very high number of incidents of suspicious transactions, which flow through the banking system. Also, a new Act, the Protection of the Constitution and Democracy and Terrorism and Related Activities Act 33 of 2004 (POCDATARA), which seeks to combat the financing of terrorism, places an even bigger responsibility on banks to report terrorist financing.

There is no doubt, that these AML financial investigations place a very heavy burden on the banks' manpower and budget. However, a more sophisticated approach to investigating dirty money flowing through the banking system is required and banks lack the manpower to analyse millions of transactions, any of which could be a money laundering transaction (Searchspace Ltd, 2002:1).

However, there are advanced accounting software and AML systems for banking available, which can assist in analysing and detecting many possible proceeds of crime and money laundering transactions by using automated transaction alert-generating systems. One should bear in mind, though, that these AML investigative systems are able to detect, alert banks to, and prevent potential money laundering schemes depending on the quality of the data collected by the bank, and the capabilities of the tools that are tasked with analysing the data (Sanjaya, 2005:10).

In addition, this rise in STRs reported to the FIC will definitely increase the workload for the SAPS. This is because the FIC may not investigate these STRs made by the banks; it may analyse and process this financial data, but must refer these STRs to a law enforcement agency for official criminal investigation (Michell, 2005:11).

Consequently, just as the banks are now starting to make use of these advanced systems, the SAPS should also consider making use of advanced accounting software to assist it in analysing and investigating this rise in STRs.

To address the third research question, more detailed research on how to use advanced accounting software as an investigative tool was conducted and is discussed in depth in Chapter 4.

CHAPTER 4:
UTILISING ADVANCED ACCOUNTING SOFTWARE TO TRACE PROCEEDS OF CRIME IN BANK ACCOUNTS

4.1 INTRODUCTION

How much human thought can go into monitoring 30 million transactions? (Searchspace Ltd, 2002:2). Banks simply cannot employ enough people to do that, and the SAPS only has a few financial investigators, with limited time, limited resources and an overload of cases. However, there is software that can analyse each transaction, and decide the risks and potential actions needed (Searchspace Ltd, 2002:2). Although the use of advanced algorithms to catch criminals may sound far fetched, financial institutions face little alternative since they lack the manpower to analyse millions of transactions, any of which could be money laundering transactions (Searchspace Ltd, 2002:2).

4.2 ADVANCED ACCOUNTING SOFTWARE

To control the business documentation environment, accountants instituted the so called paper trail or audit trail (Bologna, 1995:177). In essence that control measure requires that all business transactions be entered into journals and be supported by paper documents, such as cancelled cheques etc. (Bologna, 1995:177). Electronic versions of business records were then implemented and electronic computers were first introduced for commercial use in the US in the mid-1950s (Bologna, 1995:59). Accounting spreadsheets started out as electronic versions of hard-copy accounting worksheets with one purpose: simple row-and-column arithmetic (Chester, 1994:25).

The advent of the computer brought with it some very useful applications for investigators (Bologna, 1995:59). For example, locating assets (money) in the manual era took hours and hours and

wore out one's eyesight and patience (Bologna, 1995:59). In contrast, accounting computer software allows the investigator to drill down into volumes of financial data. According to Bologna (1995:186), these accounting systems are a natural progression from manual accounting systems.

Below, the researcher discusses which of these accounting systems can be used to capture, analyse and investigate suspicious transactions, proceeds of crime transactions, and money laundering transactions. First i2 Analyst Notebook is discussed, then the advanced financial analysis functions of Excel Accounting; thereafter, more advanced automated systems, such as Mantas Inc. and Searchspace-Fortent AML system are discussed.

4.2.1 i2 Ltd Analyst Notebook

This analytics system can be used for analysing data in any complex matter. According to i2 Ltd (2007:1), their Analyst Notebook system has a range of capabilities that allow the forensic investigations' specialist to:

- Effectively store and retrieve volumes of disparate data; and
- Use the sophisticated database solution for capturing, controlling and analysing multi-source data in a secure environment.

The i2 iBase is specifically designed for analysts and investigators, and incorporates a range of powerful functions tailored to the needs of these specialists. Once the data is captured, a wide range of analytical and query options are available to analysts and investigators (i2 Ltd, 2007:1). The sections below describe the functions which can be used to analyse financial data.

4.2.1.1 i2 iBase 5 Automatic Charting

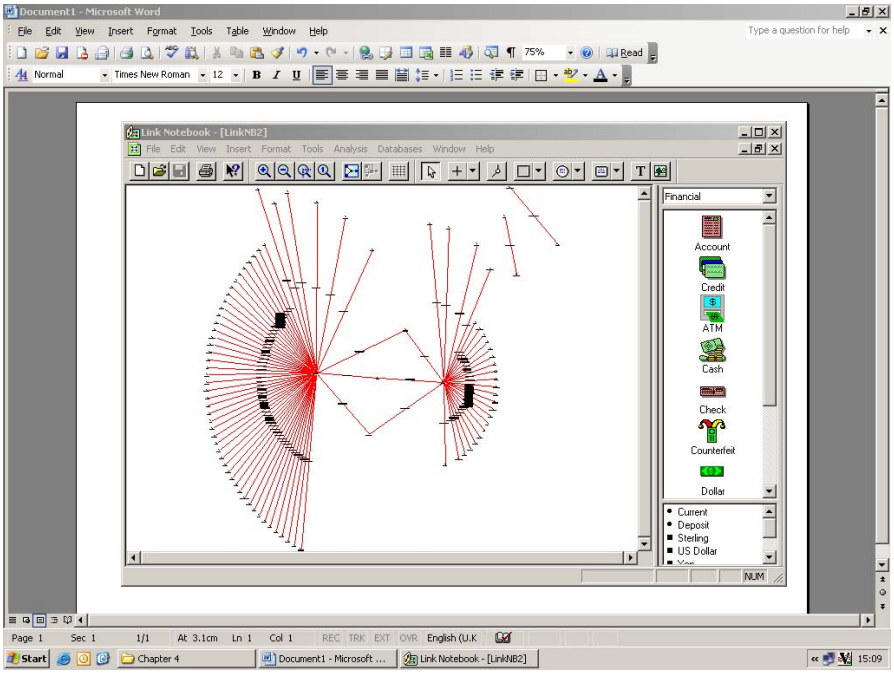
According to i2 Ltd (2007:1), the seamless integration with i2 Analyst Notebook allows the investigator to analyse data manually or to

generate link and timeline analyses from an iBase database automatically.

The financial analysis and automatic charting can be done after the financial transactions are captured in “text” format and than imported into the charting toolbox. The function automatically links entities connected in a graphical format. All information with regard to account numbers can be captured into the Analyst Notebook system and it will display how much money goes into which account (Respondent 19, 2007).

Figure 4.1, below, is an example of i2 Analyst Notebook Automatic Charting. This function can assist the investigator with the analysis of complex transaction structures.

Figure 4.1: i2 Ltd IBase 5-Automatic Charting screen shot



Source: i2 Limited (2007:1)

This function of Analyst Notebook can be used to analyse transactions flowing between several parties. Once the transactional data is inputted into the system, the charting option draws links between

subjects that have sent to and received money from each other. For example, the Analyst Notebook chart above displays a chart which depicts money transactions from several subjects to one person; the red line links money transfers from several subjects in the outer ring towards one subject in the middle of the ring. In Figure 4.1, above, the system has identified two major receivers which received transactions. This is displayed as two groups: one group of senders and one receiver is on the left; there is also one group of senders and a receiver on the right ring. The money transfer chart also indicates that the two main receivers in the middle are connected. This function can be used to trace proceeds of fraud that are, for example, being transferred among several subjects.

4.2.1.2 i2 iBase 5-Transaction Analysis

Analyst Notebook is the perfect financial tool for interrogating large financial databases and drawing graphical links between transactions (Respondent 6, 2007). This function represents transactions, such as bank transfers and telephone calls as links placed in chronological order (i2 Ltd, 2007:1).

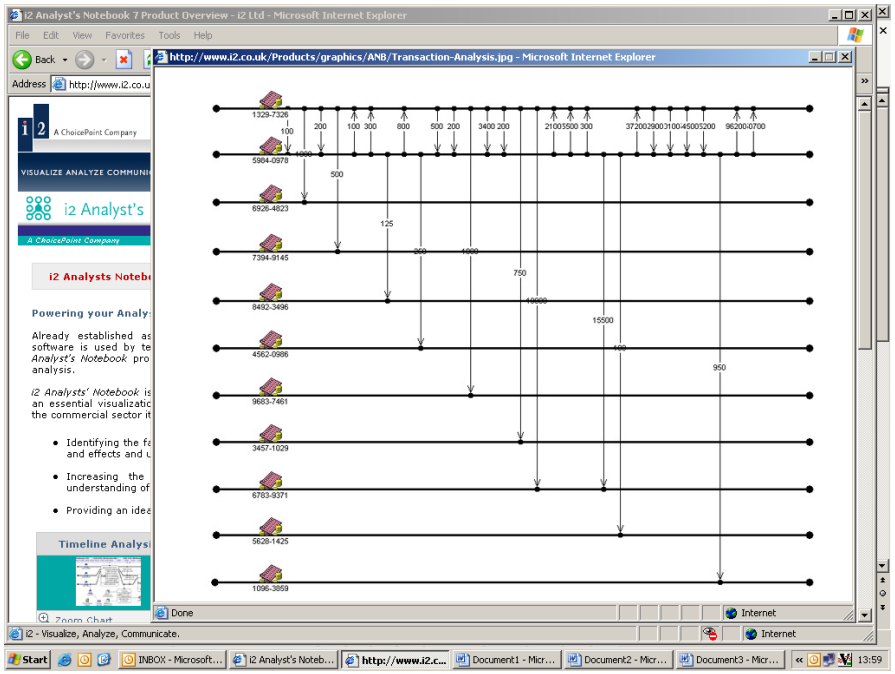
During an analysis, it is very easy to get confused with the hundreds and sometimes thousands of transactions from account to account and sometimes country to country. The figures in a normal bank account statement can also confuse the investigator at stages because they are a mixture of debits and credits. Analyst Notebook breaks the information up and automatically organises transactions chronologically and makes links between transacting parties (Respondent 19, 2007).

In addition, this function is very useful for investigating proceeds of crime and money laundering transactions because it indicates the flow of transactions in a chronological order and any person reading it can see clearly what the sequence and flow of transactions are (Respondent 19, 2007).

This makes it easier to identify the source of funds and the stage at which the funds entered the bank account. This is very important for following and maintaining the chain of evidence, which will show the links between bank accounts (Respondent 19, 2007).

Figure 4.2 displays the transaction analysis function. To explain, Figure 4.2 indicates a flow of transactions from one account to 11 other accounts. The flow of transactions starts at the top line, which represents one account, flowing downwards into other accounts, following the arrows. The arrow tip indicates where the money landed. The red icon on the left represents an account, and the account number is cited below the red icon on the left-hand side of the screen. The amount which was transferred is provided between the start of the arrow and the tip of the arrow below.

Figure 4.2: i2 Ltd IBase 5-Transaction Analysis screen shot



Source: i2 Limited (2007:1)

This system can interrogate hundreds of links in one sheet. It must also be noted that the financial toolbar in the top right-hand side of the automatic charting window screen shot makes provision for the money

laundering investigator to choose the type of banking facility that was used, such as an ATM transaction, cheque account, or cash transaction, or even whether the transaction involved counterfeit money or cheques (Respondent 6, 2007). The system also allows the financial investigator to choose from the icon list what type of currency was involved; i.e. SA(R), US($), UK(£) or EU(€) (Euro) (Respondent 6, 2007).

i2 Ltd Analyst Notebook is used during investigations by two of the 30 respondents from the sample. i2 Analyst Notebook can be used on a desktop computer or laptop and does not have to be connected to any other systems. This i2 Analyst Notebook financial investigative system is available to law enforcement and to financial services practitioners.

4.2.2 Excel-Microsoft

Most accountants and the forensic audit firms use Microsoft Excel to conduct financial modelling, to prepare financial statements and financial reports, and to conduct financial analysis and forensic accounting (Respondent 10, 2007).

The Excel program has various financial accounting fields, and many banks and financial companies use this program to store financial data to interrogate and analyse their flow of funds (Respondent 10, 2007).

With the Excel advanced accounting program, for example, the auto-transaction filtering and data-sorting functions can be used to trace proceeds of crime (Respondent 9, 2007). The Excel accounting program can be applied as a financial analysis and investigative tool to trace proceeds of crime and money laundering transactions (Respondent 10, 2007).

The financial accounting functions most relevant to tracing proceeds of crime transactions and money laundering transactions are discussed below.

4.2.2.1 Excel Accounting spreadsheets

Excel spreadsheets started out as electronic versions of hard-copy accounting worksheets with one purpose: simple row-and-column arithmetic (Chester, 1994:25). According to Chester (1994:25), the Excel spreadsheet is the main workspace for any financial analysis or accounting calculations in the program. These programs have evolved dramatically over the past decade, and are one of the most widely used categories of software products. Excel has long been the leading graphical spreadsheet (Chester, 1994:25).

From a practical auditing and investigative perspective, this is the main workspace for a financial audit or investigation. The spreadsheet is used to capture all financial records, such as bank account numbers, branch codes, and any other relevant financial data as required. Each spreadsheet has a workbook embedded in it and this workbook can have many tabs to navigate between workbooks (Respondent 10, 2007).

The workbook also has toolbars located at the top and the bottom of the workbook. These toolbars contain the main functions used for calculations, formatting values and other advanced accounting features, such as transaction filtering, financial data sorting, custom auto-filtering options and advanced charting, which can be used for financial auditing and financial investigations (Respondent 10, 2007).

The best way to use the accounting functions are to set up an Excel spreadsheet, which will be the place where the investigator can capture and store all financial data. The various fields can be populated daily as the forensic investigation progresses. As the investigator collects more investigative data, such as bank account numbers, balances and transfers to other bank accounts, more links and patterns can be picked up if all the financial data is in one database (Respondent 10, 2007).

4.2.2.2 Calculations with Excel formulas

When analysing a suspect's bank account for money laundering transactions, it is always important to ensure that the correct calculation is made during the financial investigation process. The most basic mistake is the incorrect calculation of totals. It is therefore of utmost importance that when the investigator captures amounts from any source, i.e. bank account statements, deposit slips or cheque deposits, he ensures that the amount on the source document is exactly the same amount that is captured in the Excel spreadsheet (Respondent 10, 2007).

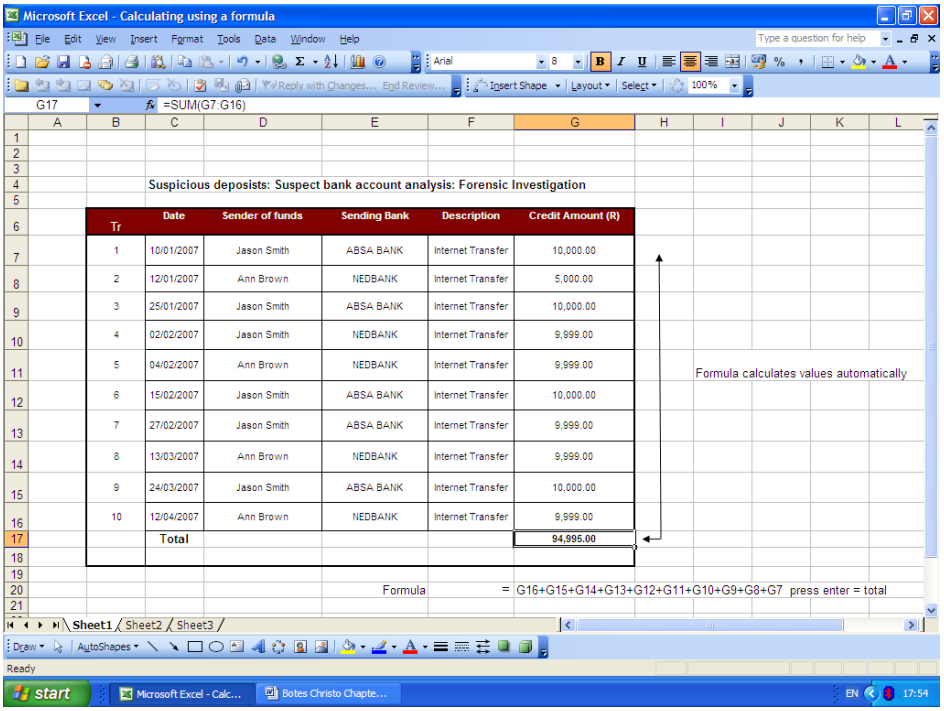
After the spreadsheet is drafted, detailing a heading and exactly the same amounts from the bank account statements, then the flow of funds can be calculated (Respondent 10, 2007). Large spreadsheets with hundreds or even thousands of transactions can be calculated using the accounting formula provided below, according to Respondent 10 (2007).

For example, according to Respondent 10 (2007), the analyst should select the cell right under the amounts that must be calculated, for example:

Enter =G16+G15+G14+G13+G12+G11+G10+G9+G8+G7 *press* "enter"; this will automatically calculate all the amounts and display a total. Figure 4.3 below provides a spreadsheet screen shot of the formula calculation.

In Figure 4.3 cell G contains all the amounts which need to be calculated; for this reason, the calculation formula will be made up of all values in cell G, and cells G7 to G17 will be calculated with the formula (Respondent 10, 2007). After "enter" is pressed, then the program will automatically calculate all the amounts in cell G and display a total.

Figure 4.3: Calculating using formulas – Excel 2003 – screen shot



Source: Respondent 10 (2007)

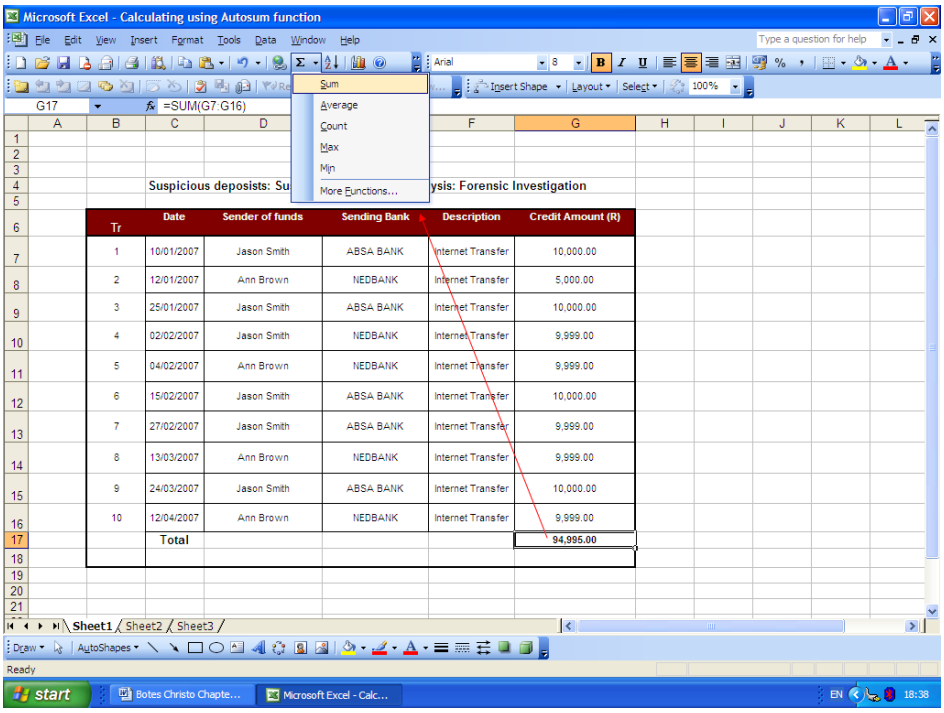
4.2.2.3 Calculating with Excel Autosum

AutoSum function allows the money laundering investigator to calculate up to 65,536 different financial data entries in a bank account or any other financial record with the click of one button; the advanced accounting program “runs” the figures itself and can calculate the totals of 65,536 rows in a few seconds (Chester, 1994:19).

Activating AutoSum to calculate flow of funds can be done by selecting the cell right under the amounts that must be calculated. The investigator should left click on the Autosum icon (Σ) in the top toolbar; a scroll down menu will appear. The investigator should then left click “Sum”. AutoSum will automatically calculate all the amounts in the various cells (Respondent 10, 2007).

Figure 4.4 provides for a systems screen shot, displaying an AutoSum calculation of ten credit transactions.

Figure 4.4: Calculating using AutoSum – Excel 2003 – screen shot



Source: Respondent 10 (2007)

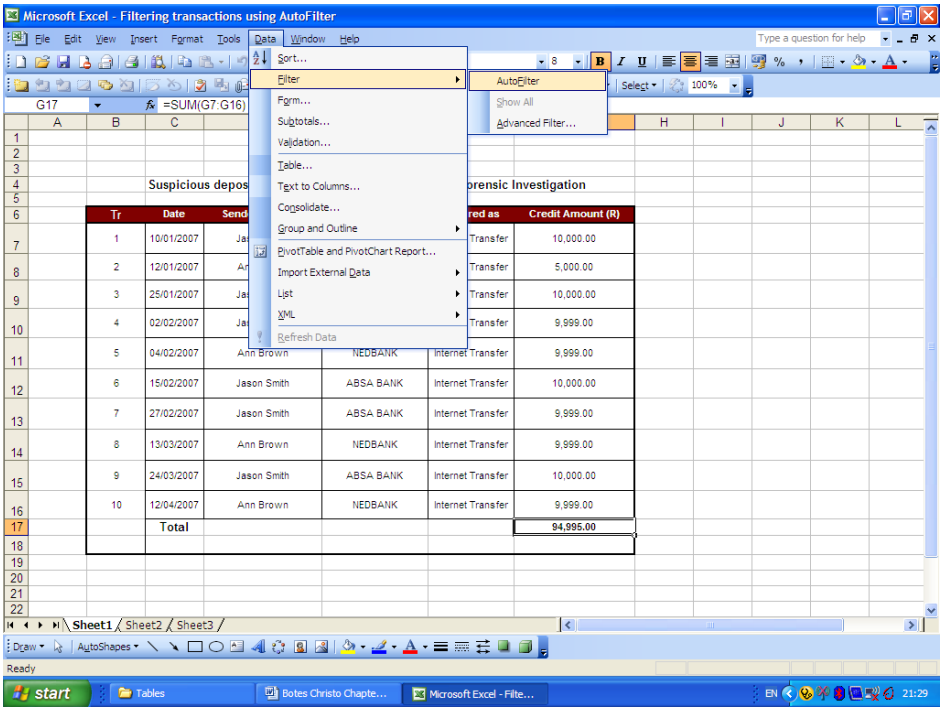
4.2.2.4 Excel Accounting spreadsheets with AutoFilter

It is always very difficult to extract certain transactions from a list of a few hundred transactions, or from a list of a few thousand transactions. For example, how long will it take a banker or a police investigator to analyse 1,000 transactions one by one? This analysis can be done in a few seconds with the AutoFilter function (Respondent 10, 2007).

In financial services transaction filtering and Auto Filter are often used to filter out suspected proceeds of crime and money laundering transactions (Respondent 6, 2007). In a nutshell, what happens is that this function of Excel is used to data mine through many different transactions in order to filter out irrelevant transactions, and to expose high-risk transactions, such as structured transactions (Respondent 6, 2007).

These transactions can be highlighted, colour coded or totally extracted from the list of 1,000 transactions and placed in another worksheet. Once the investigator activates the AutoFilter function in the Excel accounting worksheet, the function will run an automatic search through the 1,000 transactions in the worksheet. It will filter out all other transactions that are not in the filtering path and only display the requested transactions (Respondent 10, 2007). Figure 4.5 indicates how AutoFilter is activated within an Excel accounting spreadsheet.

Figure 4.5 Filtering transactions with AutoFilter – Excel 2003 – screen shot



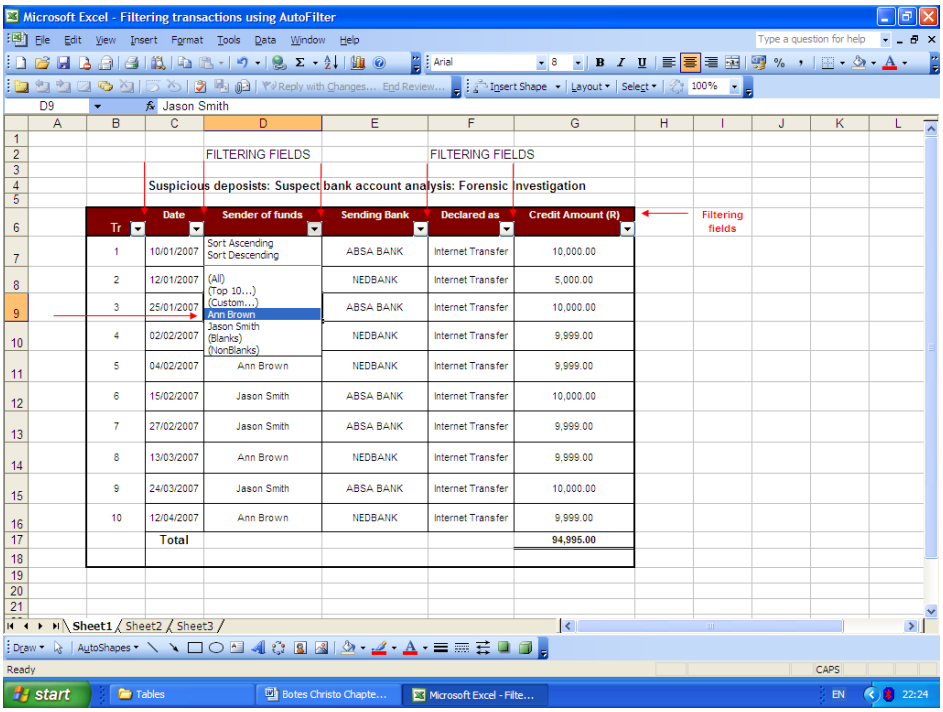
Source: Respondent 10 (2007)

As explained above, once the AutoFilter function is activated, a whole range of financial filtering options are displayed horizontally across the accounting spreadsheet. This means that the investigator investigating money laundering can now choose to filter any part of the financial spreadsheet (Respondent 10, 2007).

The investigator may want to focus on analysing transactions from one depositor in the spreadsheet, for example Ann Brown. Whilst the AutoFilter function is activated, the investigator must click on the sender of funds filtering tab, and scroll down the tab, and than clicking on Ann Brown. The AutoFilter will automatically filter out all transactions made by Ann Brown (Respondent 10, 2007).

See Figure 4.6 for a screen shot example of how the AutoFilter function works.

Figure 4.6: Filtering transactions with AutoFilter – Excel 2003 – screen shot



Source: Respondent 10 (2007)

The money laundering investigator can also filter out deposits from certain months, or even filter out a specific bank or even a specific deposit, such as an Internet transfer, cheque deposit or cash deposit. The AutoFilter and Custom AutoFilter function can also be used to trace transactions that are made under the cash threshold, which form cash threshold transactions (Respondent 10, 2007).

For example, if a person walks into a bank and deposits R 10, 000.00 in cash or more, then the bank must report this transaction to the FIC as a "cash threshold transaction". However, money launderers know this and deliberately make smaller transactions and make payments just under the cash threshold amount in order not to be reported to the FIC (Respondent 10, 2007).

This money laundering technique is known as "structuring" (Wikipedia, 2007:1). "Structuring a cash deposit" is banking industry jargon used to describe the act of splitting a large financial transaction into smaller transactions to avoid scrutiny by regulators or law enforcement. It is commonly used in the context of money laundering and has been known to appear in official Federal criminal indictments (Wikipedia, 2007:1).

The AutoFilter or Custom AutoFilter Function can be used to identify these structured transactions. As explained above, if the police investigator is trying to identify money laundering transactions, or transactions that are designed to evade cash threshold reports (CTR) made by a banker, than an AutoFilter or Custom AutoFilter can be applied to a few hundred or even a few thousand transactions (Respondent 10, 2007).

The investigator can use AutoFilter by clicking on the scroll down arrow in the AutoFilter section of the amounts column and then clicking on "sort data A – Z". This will sort all the financial transactions from R0 to whatever the biggest amount is (Respondent 6, 2007). The transactions will be automatically sorted and all transactions of just under R 10,000, i.e. R 9,999 or R 9,500 or in whatever denomination the money was structured, will be identified and colour coded much more easily. At least 65,500 transactions can be sorted from the biggest to smallest amount, as described above, in a few seconds (Respondent 6, 2007).

To conclude this discussion on Excel, this accounting program is used during investigations by three of the 30 respondents from the sample. Excel accounting can be used on a desktop computer or laptop and does not have to be connected to any other systems. The above-mentioned Excel accounting program is available to financial services and to law enforcement.

There are even more advanced automated accounting systems which can be used to trace proceeds of crime through bank accounts. These systems, which are discussed below, are used by the banking sector to detect and investigate suspicious transactions, such as fraud and money laundering.

These automated systems are not available to police officers for investigation; this is because these systems are connected to the banks' transaction systems and only bankers who are responsible for AML will use these systems for financial investigations.

In addition, it must be emphasised that the researcher specifically cites certain respondents from the sample in the discussion below. This is done because these respondents are bankers who are exclusively involved in detecting financial irregularities, such as proceeds of crime and money laundering on behalf of their banks and are highly specialised in the use of these automated AML systems.

They are not police investigators, but conduct highly specialised financial investigations within financial services, such as banks and the Johannesburg Stock Exchange.

4.3 AUTOMATED ADVANCED ACCOUNTING SOFTWARE

Automated advanced accounting systems are used for monitoring transactions within the banking environment. With today's banking systems, transactions can move from one country to another with the

click of a button (Respondent 9, 2007). Internet banking, voice activated transactions, chip and pin card transactions, and cell phone banking transactions are the reality of today's high tech banking environment (Respondent 9, 2007).

As the banking technology increases, more financial systems' weaknesses and financial risks are exposed and it becomes more difficult to control paperless banking transactions (Respondent 9, 2007). Consequently, it becomes increasingly complex and difficult for bankers and police investigators to trace proceeds of crime transactions and money laundering transactions (Respondent 9, 2007).

For example, a money launderer can now use Internet banking or cell phone banking to transfer money to many different bank accounts in a day. This dirty money that moves from Internet bank transfer to Internet bank transfer gets cleaner and cleaner the more it is transferred through a series of bank accounts (Respondent 9, 2007).

This process gets so complex at stages that even some of the most experienced bankers do not know what the actual source of the money is, or where it was integrated into the banking system (Respondent 9, 2007).

This makes it necessary to use analytics, with advanced accounting capabilities embedded into the analytics system, that can assist in identifying and investigating these suspicious transactions, in real-time, as they are occur. The so called automated transactions monitoring systems or AML systems are used to address this complex money laundering issue (Respondent 9, 2007).

The other respondents of the sample, including police investigators and the financial services respondents, replied to the question: "can you explain which advanced accounting software can be used as a forensic

investigative technique, to trace the reintegration of proceeds of crime into the banking system?" as follows:

- Five out of the 30 respondents described an advanced accounting software and AML investigative system and how it is used to trace proceeds of crime and money laundering transactions; this component of the sample also mentioned i2 Analyst Notebook, Excel Accounting, Mantas Inc and Searchspace-Fortent; and
- Twenty-five of the 30 respondents reported that they did not use and do not know of any such advanced accounting software and AML investigative systems.

The AML investigative systems and techniques that are discussed below focus on the automated filtering of transactions, high-risk names and financial scenarios, to automatically detect possible proceeds of crime and money laundering transactions as they occur.

4.3.1 Using Mantas Inc. for financial investigation

In the past, firms have analysed historical data to detect money laundering and predict potential losses. Unfortunately, that approach does not account for new problems and, more importantly, provides no ability to act to prevent loss. It simply allows firms to account for losses (Mantas Inc, 2003:15). However, there are financial investigative systems such as Mantas Inc, which use unique automated approaches to uncovering and alerting management to complex operational risks such as identity theft, money laundering and price manipulation (Mantas Inc, 2003:13).

By using advanced techniques, such as link analysis, sequence matching, peer comparison, rules matching, and text-mining algorithms to detect patterns within voluminous data, Mantas Inc. systems are used today to reduce litigation and fraud risk (Mantas Inc, 2003:15).

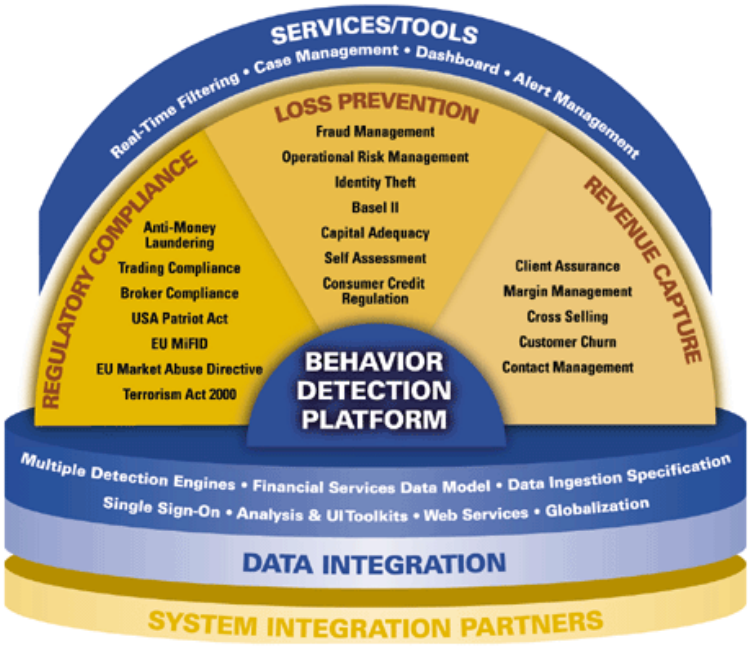
Mantas Inc. behaviour-detection techniques, such as data mining, data visualisation, and statistical analysis have been used successfully in the financial services industry. Mantas Inc. solutions have been used by the US National Association of Securities Dealers Automated Quotations (NASDAQU) exchange to monitor trends and by several banks, such as Merryl Lynch Bank, to analyse transactions and equity trades (Mantas Inc, 2003:3).

Some market leaders in the world use Mantas Inc. solutions for their AML detection and investigation. Banks, such as Citibank use the deep computing expertise, the behaviour detection techniques, and real-time analytics to ensure best practice in risk management and operations (Mantas Inc, 2004:5).

According to Respondent 4 (2007), who is a senior technical adviser at the Johannesburg Stock Exchange (JSE), a similar automated transaction monitoring system is used at the Johannesburg Stock Exchange. This system (JSE SETS ALERTS SYSTEM) assists the Johannesburg Stock Exchange in identifying insider trading activities and also how much the values of these trading deals were (Respondent 4, 2007).

The Johannesburg Stock Exchange uses accounting software which uses advanced algorithms to identify market abuse and unusual trading patterns, and conducts forensic investigation and pro-active detection of market abuse, such as insider trading in the Spot Equities, Financial derivatives, Agricultural derivatives, and Yield X markets (Respondent 4, 2007). Figure 4.7 is an example of a similar automated transaction-monitoring system.

Figure 4.7: Mantas Inc. Behaviour detection platform



Source: Mantas Inc (2004:2)

The Mantas Inc. behaviour detection platform (see Figure 4.7) has other functionalities besides the AML angle; however, the Mantas automated scenario detector, Mantas scenarios and Mantas features for AML investigations are further discussed below.

4.3.1.1 Mantas Inc. automated scenario detector

Bankers can use this function to detect suspicious transactions that might be proceeds of crime transactions or money laundering transactions automatically. Mantas Inc. AML has embedded in the authorisation path, pre-programmed scenarios that attempt to match financial transactions flowing through the bank account, with the pre-programmed scenarios. The following list of scenarios represents a portion of the behaviours that can be identified (Mantas Inc, 2004:2).

4.3.1.1.1 Mantas Inc. Scenarios – AML investigations

According to Mantas Inc. (2004:2), its AML system and automated transaction monitoring tool use these indicators when identifying suspicious transactions for further investigation:

- High-risk geographies and entities

  According to Mantas Inc. (2004:2), it can automatically detect transactions to high-risk countries and entities. Mantas Inc. Real-time Sanction List Filtering meets the most sophisticated real-time filtering of names' requirement.
- Hidden relationships

  It can detect networks of accounts, patterns of funds' transfers, and patterns of recurring transactions (Mantas Inc, 2004:2).
- Anomalies in behaviour

  It can detect changes in financial transaction behaviour and rapid movements of funds (Mantas Inc, 2004:2)
- Other money laundering behaviour

  It can detect single or multiple cash transactions, structured transactions, or avoidance of (CTR) cash threshold transactions, large reportable transactions, checks with sequential numbering, and anomalies in ATM and bank card activity (Mantas Inc, 2004:2).

When a scenario is detected by Mantas Inc, it will generate an automatic alert, which can be viewed in the alert assignment queues of the program (Mantas Inc, 2004:3).

4.3.1.2 Mantas Inc. Features – AML investigations

The features mentioned below are used for AML investigations. The alert generation, alert workflow, research workflow, and reporting workflow are discussed:

- Alert generation

  This function identifies money laundering/suspicious activities and generates an automatic alert. Other alerts are generated on the basis of certain scenarios. The system can extract hidden extended relationships from text of wire transactions and messages (Mantas Inc, 2004:3). The system also uses watch list and fuzzy name matching to identify high-risk customers,

accounts and entities. In essence, this function applies a wide range of scenarios to create alerts that get assigned to a specialist banker for further investigation.

- Alert workflow

  Mantas Inc. (2004:3) states that managing alerts of suspicious transactions and the re-assignment of alerts for further investigation can also be controlled by the system.

  According to Mantas Inc. (2004:3), a range of alert workflow for investigating options is available; however, the following are the most relevant:

  - Filter and sort the displayed alerts;
  - Automatically alert assignment to queues, individuals, or groups;
  - Score alerts for investigation prioritisation on the basis of risk;
  - Analyse the reason for and details of alert;
  - View the related background data for an alert;
  - Capture the full audit trail of activities involved in alert resolution;
  - Facilitate supervisory approval for an action on an alert;
  - Export alert information to facilitate automatic population of case management system and regulatory reporting such as STRs/SARs.

- Research workflow

  This function assists the banker with the actual research after he has received the automated alert, such as retrieving and analysing the alert history for a specific account or customer (Mantas Inc, 2004:3). The actual research involves researching and analysing contextual and summary information for a specific account and creating user-initiated alerts to respond to ad-hoc investigation (Mantas Inc, 2004:3).

- Reporting workflow

  This involves analysing the reason for closing alerts by business units or individuals. For example, the system could generate an automated alert on the basis of a specific transaction. Then, after an initial analysis, a banker may decide to close the alert and sign it off as not suspicious because he thinks the transaction is not money laundering. This workflow process of risk-based decisions is captured. The program allows for the capture and track user sign-off on the disposition of alerts assigned to a business unit and for the view of a summary of alerts generated against specific focuses, accounts and customers (Mantas Inc, 2004:3).

  The Mantas Inc. system is not used by any of the respondents from the sample. However, one respondent uses a system which is quite similar to the above-mentioned system. As mentioned above, this system is mostly used by the large banks. The Mantas Inc. system is not available to police investigators, but is available for financial services such as banks because it needs to be connected to the banks' transaction systems.

4.3.2 Using Fortent Ltd for financial investigation

An AML system, such as Searchspace Ltd (Fortent Ltd), is an integrated AML compliance platform which allows a bank to monitor transactions and manage its day-to-day AML regulatory requirements (Respondent 9, 2007).

Fortent Ltd is a provider of enterprise-wide risk and compliance solutions (Fortent Ltd, 2006a:2). Fortent Ltd was previously known as Searchspace Ltd, and changed brand names on 28 June 2006 (Searchspace Ltd, 2006:1).

The Fortent Ltd AML system, AML Sentinel, is mostly used in the banking environment. Part of the AML Sentinel design is the unique

AML Case Investigation System (CIS), which is an easy-to-use graphical front-end to its Intelligent Enterprise Framework, which is designed to be used by money laundering investigators to help them efficiently investigate cases of high-risk activity that have been identified by the framework (Searchspace Ltd, 2004b:1).

This system provides an infrastructure to support a multi-person, multi-location investigation process. It is designed to make the human investigation process as efficient as possible by pre-calculating all the information that might be required in an investigation up-front to avoid the need for real-time queries during the investigation process (Searchspace Ltd, 2004b:1).

Cases can be manually generated or automatically by the Searchspace Automatic Investigations Engine, which has lists, rules, and automatic components (Searchspace Ltd, 2004b:1). The AML Sentinel CIS, and the technique a banker can use to identify proceeds of crime transactions, is discussed below.

4.3.2.1 The AML Sentinel Case Investigation System

AML Sentinel CIS interfaces directly with a bank's transactions system. The Fortent Ltd system can be implemented in banks with a transaction volume of up to 50 million transactions a day (Searchspace Ltd, 2002:2). The AML system automatically organises and presents all available information relating to detecting unusual, suspicious, and high-risk activity (Searchspace Ltd, 2002:2). It generates automatic alerts on a daily basis and the whole case, from creating an alert, to closing the alert or reporting it to the local Financial Intelligence Unit (FIU), is investigated through this system. The Fortent Ltd CIS is discussed below.

According to Searchspace Ltd (2004b:2), its AML Sentinel CIS consists of 12 screens, which display information relevant for detecting

suspicious transactions, possible proceeds of crime, and money laundering transactions. This system is discussed below:

4.3.2.1.1 The Summary of Cases Screen

The investigating banker will log on to the system and will see a list of cases for his or her attention. Each case has a unique ID alert and a risk score, which is a high-level representation of the degree of risk the activity may represent to the bank (Searchspace Ltd, 2004b:2).

4.3.2.1.2 The Customer Summary Screen

To investigate the case further, the investigating banker can double-click on a case in the Summary of Cases Screen. This then accesses the case and drills down into more detail on why an alert was generated and the background of the case, such as customer's name, address and various accounts (Searchspace Ltd, 2004b:3). An example of an alert might be: "cash structuring" and unusual activity in the customer retail banking account.

The alert "History" pane shows the action that has been taken and the comments that have been made already during the bank's previous investigation of the case. The investigating banker can see in the "Related-Alerts" pane on the same screen whether any cases have been raised previously on an account (Searchspace Ltd, 2004b:3).

4.3.2.1.3 The Account Summary Screen

For further investigation, the banker can double-click on any of the accounts in the "Reason for Alert" pane of the Customer Summary Screen (Searchspace Ltd, 2004b:4).

The Account Summary Screen shows the product type, the branch where the account resides, the date the account was opened, and other account-related information that may be relevant to the investigation. The screen also gives more information on reasons for

the violation of a “Retail Cash Structuring Scenario” (Searchspace Ltd, 2004b:4).

4.3.2.1.4 The Events Summary Screen

In this system, cases are generated automatically (Searchspace Ltd, 2004b:5). The automatic detection system has three components (Searchspace Ltd, 2004b:5):

- **The Transaction Filter,** which monitors transactions against known high-risk entities on embargo lists;
- **The Business Logic Unit (BLU),** which monitors customer activity for known money laundering scenarios;
- **The Security Blanket,** which is a more automated component that does an automated risk assessment of each customer’s activity to identify high-risk activity where the laundering pattern does not necessarily conform to any of the scenarios programmed into the system.

Because money laundering is typically a complex series of transactions of different transaction types in several accounts over a period of time, the AML system must have a holistic and contextual view of customers’ behaviour (Searchspace Ltd, 2004b:5).

In essence, the system checks each customer’s use of each product and each transaction type, comparing current activity to activity the system has seen in the past (Searchspace Ltd, 2004b:5). If a customer uses an account in an unusual way or in a way that is unusual for customers like this, then all of those results are shown on this screen. Events are also generated when the customer uses a product that he has never used (Searchspace Ltd, 2004b:5).

The above-mentioned functions of the automatic detection system form an example of AML investigative systems that can be used to trace proceeds of crime and money laundering transactions. These systems

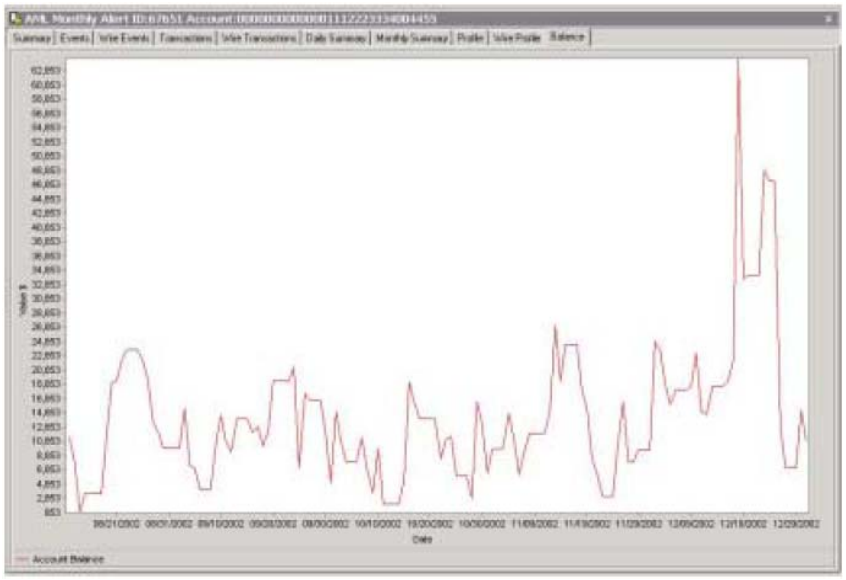
can assist a bank to report these transactions to the FIC, which, will also make the bank compliant with AML legislation.

The Fortent Ltd AML System can also assist in regulatory reporting, such as producing a section 29 report to the FIC. It just depends on whether this functionality is pre-programmed into the bank's AML system (Respondent 9, 2007).

4.3.2.1.5 The Balance Summary Screen

This screen of the system allows the investigator to have a graphical visualization of the balance over time on the Balance Summary Screen, which is shown in Figure 4.8 below (Searchspace Ltd, 2004b:7). The graphical view makes it much easier for the investigating banker to identify big changes or an upsurge of money coming into the account, as seen on the right-hand side of the Balance Summary Screen below.

Figure 4.8: The Balance Summary Screen (AML Sentinel)



Source: Searchspace Ltd (2004b:7)

This point of integration into the bank account can mean that the graph can be used to pin-point a suspicious transaction for reporting to the FIC and this transaction may be further investigated to ascertain the

source of the funds and whether the money was laundered further into more accounts.

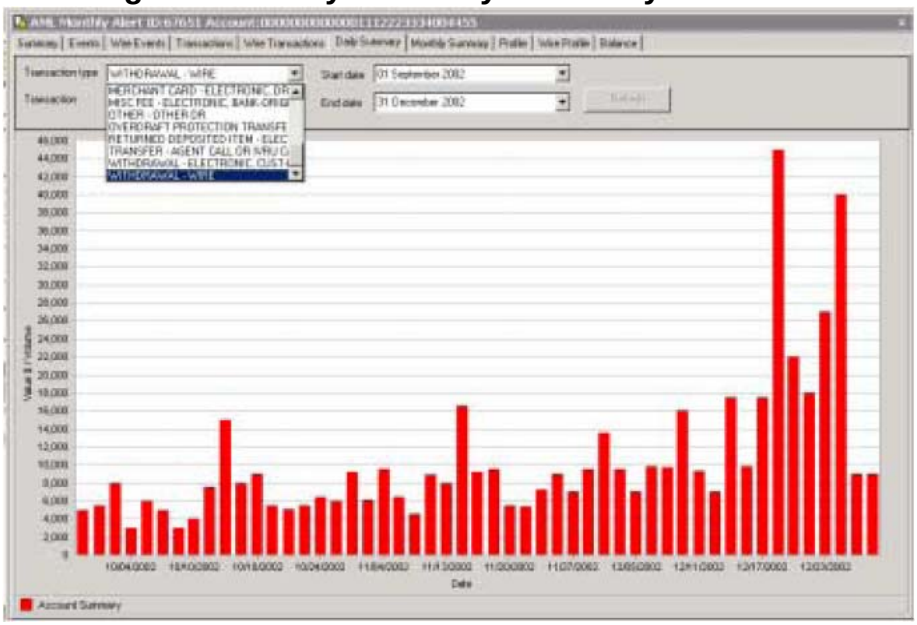
4.3.2.1.6 Account Profile Screen

This system keeps a record of each account's typical use of each transaction type. This information can be viewed in the Account Profile Summary Screen (Searchspace Ltd, 2004b:8). This screen also gives the investigator a quick summary of the types of transactions that this customer is making in this account (Searchspace Ltd, 2004b:8).

4.3.2.1.7 Daily Summary Tab Screen

The daily Summary Tab Screen shows a graphical representation of account activity by transaction type over the recent period. Figure 4.9 below shows the wire withdrawals by value of an account (Searchspace Ltd, 2004b:9).

Figure 4.9: Daily Summary of Activity Screen



Source: Searchspace Ltd (2004b:9)

This point of extraction out of the bank account, for example a wire transfer, means that the Daily Summary Tab can be used to pin-point a suspicious activity or suspicious wire transfers out of South Africa. The financial activity on the right-hand side of the screen above clearly

shows a much higher flow of funds than normal and the investigating banker can immediately focus attention on that transfer.

4.3.2.1.8 Statement Data Summary Screen

If required, the investigator can also drill down to the base transaction data normally shown on the bank statement (Searchspace Ltd, 2004b:9). This system allows the investigating banker to view the base transaction information instantly.

4.3.2.1.9 Wires Summary Screen

Normally wire transactions (swift international transactions) are considered high-risk transactions because the funds can be received from off shore tax havens or other more high-risk countries, such as Russia, Colombia or Nigeria. This screen displays all sending and receiving wire transactions (Searchspace Ltd, 2004b:10).

4.3.2.1.10 Link Analysis Screen

The information presented so far has only been relevant to the alert customer and his accounts (Searchspace Ltd, 2004b:11). It is, however, necessary for an investigator to have more information about the different links and relationships that this account might hold (Searchspace Ltd, 2004b:11).

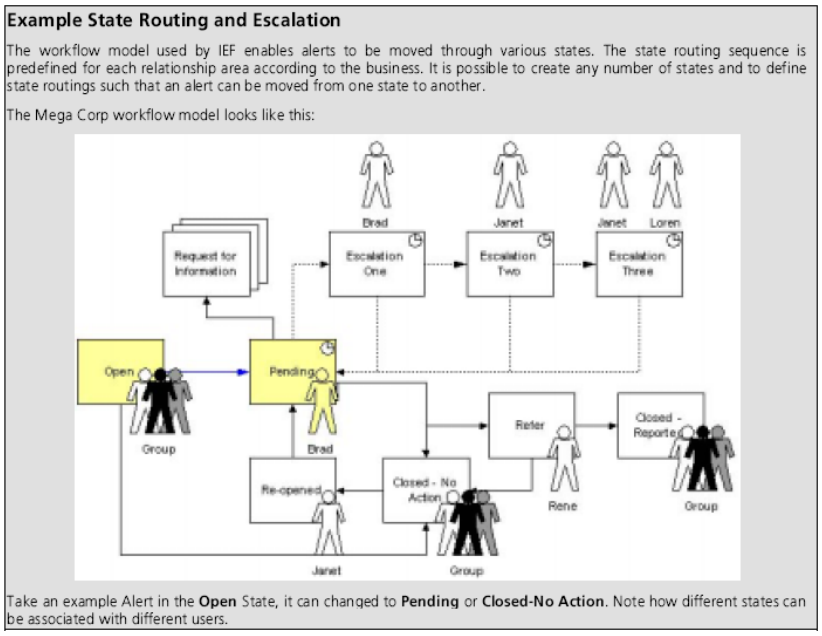
Another piece of information which is important to an investigator is the identification of any unspecified relationships in the data. This information is displayed in the Link Analysis Screen. The system can discover hidden financial relationships with another account using link analysis investigation (Searchspace Ltd, 2004b:11).

4.3.2.1.11 The Workflow Manager Screen

The system allows the investigator to take appropriate actions as a next step in the investigation (Searchspace Ltd, 2004b:12). Along the bottom of the Summary Screen is a number of workflow buttons, which allows the investigator to move the case to another state using the

Searchspace Workflow Manager, (see Figure 4.10 below). If the investigator decides the case deserves more detailed analysis, by a more senior investigator, he may press the “referred” button to send the case to a higher level (Searchspace Ltd, 2004b:12).

Figure 4.10: Searchspace Workflow Manager Screen



Source: Searchspace Ltd (2004b:12)

Figure 4.11: Workflow Buttons

Source: Searchspace Ltd (2004b:12)

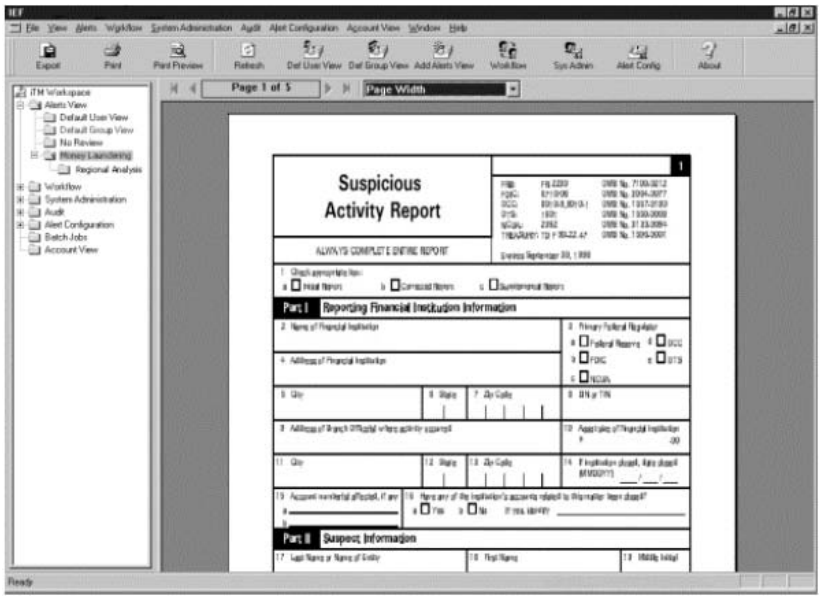
If the case is routed to another investigator, all of the history and the comments made by the investigators are automatically transferred with the case (Searchspace Ltd, 2004b:12). The Workflow Manager is shown above in figures 4.10 and 4.11.

The above-mentioned workflow functionality can also automatically route cases to a different state after a bank-determined timeout (for example five days of investigation); this is known as automatic escalation (Searchspace Ltd, 2004b:12).

4.3.2.1.12 Reporting the case to the Financial Intelligence Centre

If the investigator decides that the case should be sent to the FIC, then the investigator uses the "Report Workflow" button. When pressed, the system will auto-populate a pre-configured report for submission to the FIC (Searchspace Ltd, 2004b:12).

Figure 4.12: Electronic SAR Form Submission Screen



Source: Searchspace Ltd (2004b:12)

It must be noted here that this function is the last stage of identifying suspicious transactions that might be proceeds of crime or money laundering. Normally it takes a substantial amount of time to put together such a report, and this function, which automatically writes the suspicious activity reports, saves a lot of time. This allows the bank to conduct more financial risk investigations because the bank investigators do not have to spend time writing report after report.

In addition, the Fortent Ltd AML System is used by some of the world's biggest banks, including Commerce Bank, JP Morgan Chase Bank, Barclays Bank, Chevy Chase Bank, First Horizon National Corporation, First Hawaiian Bank, Loyds TSB Bank, Societe Generale Bank, The

Bank of New York, The Royal Bank of Scotland, and the United Bank of Switzerland (UBS) (Fortent Ltd, 2006b:2).

South Africa's biggest banks have also moved to utilise Fortent Ltd to detect suspicious activity, proceeds of crime and money laundering transactions.

Nedbank Ltd, one of South Africa's biggest banks, successfully deployed the Fortent Ltd AML case investigation system on 11 January 2006 (Fortent Ltd, 2006a:1).

ABSA Bank Ltd (a division of Barclays Bank) has also selected the Fortent Ltd AML case investigation system for its retail and correspondent banking operations (Fortent Ltd, 2005:1).

Standard Bank Ltd has also successfully implemented the Fortent AML case investigation system (Fortent Ltd, 2006b:1).

Lastly, one respondent from the sample uses the Fortent Ltd system to detect proceeds of crime in the banking environment during investigations. This AML system is not available to the SAPS because it can only be installed into a bank's financial transaction system.

Mostly banks will use this type of advanced accounting software to investigate suspicious transactions which might be proceeds of crime or money laundering transactions.

4.4 SUMMARY

Referring to the above-mentioned processes, it is clear that money laundering is a highly sophisticated and complex financial crime. It is also clear from the fines imposed on banks that proceeds of crime flowing through bank accounts and money laundering transactions can cause significant financial burdens for banks, and the reputational risk

associated with money laundering for a bank can have even worse effects in the long run.

Banks cannot afford to ignore the risks posed by money laundering, and have to take them seriously. Not taking money laundering seriously can cause significant damage to a bank's brand, and, in the long term, can cause a major drop in the share price of the bank.

Moreover, a massive fine of a few million can be imposed on the bank and cause even further damage. In a worst case scenario, money laundering can spiral out of control and South Africa can be blacklisted by the United Nations and the FATF as a Non Cooperative Country and Territory (NCCT). If this happens, South Africa will be seen as a country that is not cooperating in the combating of terrorist financing and money laundering activities, which could have a direct effect on foreign direct investment into South Africa.

The i2 Analyst Notebook and Excel advanced accounting features can be used on a desktop or laptop computer; it needs no systems' integrations, and does not have to be connected to a bank's transactions' system. These financial investigative systems have the capacity to analyse and filter transactions which will help investigators to identify proceeds of crime and money laundering transactions with great speed and accuracy.

On the other hand, the automated advanced accounting systems and AML systems which are connected to the banks' transactions' system are not available to police detectives and they are not able to work with the systems as an investigative tool, since they are part of the internal systems of various banks. The banking sector, however, can use these systems to detect, investigate and report suspicious activity, proceeds of crime, and money laundering transactions to the FIC.

Nevertheless, the police investigator can still have access to these automatically generated money laundering reports by applying to the FIC for any reports made in terms of section 29 of the Financial Intelligence Centre Act.

Chapter 5, which follows, discusses the findings and recommendations made with regard to the use of advanced accounting software to trace the proceeds of crime from underground banking into the formal banking system.

CHAPTER 5:
FINDINGS AND CONCLUSIONS

5.1 INTRODUCTION

The aim of this research report was to research how advanced accounting software can be used by police detectives, financial risk specialists and forensic investigation specialists, who are responsible for the investigation and tracing of the reintegration of proceeds of crime, from underground banking into formal banking systems (pro-active and reactive money laundering investigation), with a view to criminal prosecution. The researcher attempted to achieve this aim by utilising data such as that obtained from reviewing current literature, conducting interviews, and assessing case files. The findings of the research are outlined below.

5.2 FINDINGS

5.2.1 Findings regarding the research questions

The primary findings presented below were based on the research questions.

5.2.1.1 Underground banking

"Underground banking" is a generic term used to describe any informal banking arrangement, which runs parallel to, but is generally independent of, the formal banking system. Underground banking has long been regarded as a conduit for money laundering by criminal organisations and arguably by terrorist networks. The research established that underground banking received a substantial amount of attention from the World Bank and FINCEN after the 9/11 terrorist attacks in the US. Underground banking is seen in such a serious light by the World Bank, that it commissioned a large-scale research project

in 2003 on the issue, and even included two field visits to Afghanistan, where underground banking techniques such as hawala were researched. It was established that underground banking is active in South Africa and that several international currency smuggling groups have been dismantled by the SAPS and the Scorpions.

5.2.1.2 Formal banking

Formal banks are exposed to very high risks when proceeds of crime transactions flow through the banking system. It was established that there are approximately 33 registered South African banks and that they can be divided into the categories of: Retail Bank, Corporate Bank, Private Bank and Investment Bank. All banks in South Africa are regulated by the South African Reserve Bank (SARB) and are administered under the Banks Act 94 of 1990. Banks are also regulated by the Financial Intelligence Centre (FIC) of South Africa, under the Financial Intelligence Centre Act 38 of 2001.

It was established that banks must report suspicious transactions, money laundering transactions, and terrorist financing transactions to the FIC, in terms of Act 38 of 2001 (FICA), section 29 – Suspicious Transaction Report (STR) also known as suspicious activity reports (SARs) in the banking environment in other parts of the world. It was established that formal banks reported 44,021 STRs in the past five years (from 2002 to 2006).

5.2.1.3 Types of advanced accounting software

It was established that there are several advanced accounting software systems available which can be used as a financial investigative and analysis tool. There are accounting software packages available for financial analysis on a laptop computer and more advanced accounting and AML investigative systems for banking, which can assist in analysing and detecting suspicious transactions, possible proceeds of crime, and money laundering transactions by using automated transactions' alert-generating functionalities.

Five out of the 30 respondents confirmed that there is advanced accounting and AML investigative software available, and mentioned one of Excel Accounting, i2 Analyst Notebook, Searchspace Ltd-Fortent Ltd, or the Mantas Inc. system.

Twenty-five out of the 30 respondents, however, reported that they do not know of any such advanced accounting software and AML investigative systems.

Twenty-five out of the 30 respondents said that they had never received training in the use of advanced accounting software to trace proceeds of crime into banking systems.

From the research, it became clear that the respondents were knowledgeable about the legal aspects of money laundering. However, not many AML practitioners from the sample had the required expertise when it comes to using advanced accounting software to investigate the flow of proceeds of crime entering the formal banking system. Also, it is clear that many respondents had not received training in the use of advanced accounting software to investigate the flow of proceeds of crime entering the formal banking system.

5.2.1.4 Advanced accounting software

It was established that accounting spreadsheets started out as electronic versions of hard-copy accounting worksheets with one purpose: simple row-and-column arithmetic (Chester, 1994:25). Accounting software allows the investigator to drill down into volumes of financial data. According to Bologna (1995:186), these accounting systems are a natural progression from manual accounting systems.

It was established that advanced accounting software allows the forensic investigations' specialist to store and retrieve volumes of disparate data effectively and to use the sophisticated database

solution for capturing, controlling and analysing multi-source data in a secure environment.

The research identified financial investigative systems, such as i2 Analyst Notebook, Excel Accounting and more advanced automated systems, such as Mantas Inc. and Searchspace-Fortent AML System. It was established that i2 Analyst Notebook and Excel Advanced Accounting features can be used on a desktop or laptop computer; these programs need no systems integrations and do not have to be connected to a bank's transactions' system. These financial investigative systems have the capacity to analyse and filter transactions, which will help investigators to identify proceeds of crime and money laundering transactions with great speed and accuracy. It was established that these systems are available to police investigators and financial services' financial specialists.

On the other hand, the automated advanced accounting systems and AML systems, such as Mantas Inc. and Searchspace-Fortent Ltd AML System, which are connected to the banks' transactions' systems, are not available to police detectives and they will not be able to work with the systems as an investigative tool, since they form part of the internal system of various banks. However, forensic investigators within a banking environment can utilise advanced investigative systems, such as Mantas Inc. and Searchspace-Fortent Ltd, to trace proceeds of crime entering the banking system.

5.3 RECOMMENDATIONS

The following recommendations are made:

- The financial services, such as banks, will benefit more from using automated transaction monitoring AML systems because they administer a few million bank accounts. It is not possible to monitor and investigate millions of transactions with a few banking investigators. The banks will have to rely on the

assistance of automated advanced accounting software systems to identify proceeds of crime and money laundering transactions. Continued reliance should be placed on systems such as Mantas Inc. and Searchspace-Fortent Ltd for detailed analysis and follow-up investigations by forensic investigators within the bank. Forensic investigators within a bank can also make use of i2 Analyst Notebook and Excel Accounting to assist with the identification and reporting of suspicious transactions, proceeds of crime, and money laundering to the FIC of South Africa.

- Police investigators working with complex financial and commercial crimes, such as money laundering, should be provided with financial analysis and investigative tools, such as laptop computers, the i2 Analysis software, and Excel advanced accounting programs.

- Police investigators should be provided with ongoing training to analyse and investigate money laundering effectively and accurately with the above-mentioned financial investigative and analysis tools. These financial investigation and transactions' analysis tools can assist police detectives in analysing hundreds and even thousands of transactions in a very effective and organised way. Referring to the increasing numbers of STRs filed at the FIC, it is clear that the SAPS will be expected to investigate these growing numbers of STRs. It is, therefore, recommended that police detectives be supplied with financial investigative tools to cope with these increasing numbers of suspected money laundering incidents.

- It is recommended that the stand-alone computer (laptop), with advanced accounting software, such as i2 Analyst Notebook and the advanced data sorting and data filtering functions of the Excel financial accounting program, be used for proceeds of

crime and money laundering investigations by police investigators. The above-mentioned advanced accounting software can assist the police investigators to design their own investigative database, draft financial flow charts, create bank account number logs, and automatically calculate totals using pre-programmed formulas, which will eliminate complex calculation mistakes.

5.4 CONCLUSION

Proceeds of crime and money laundering transactions flowing through the South African banking system are a reality. Suspicious transactions are reported daily to the FIC and the number of reports submitted is growing by the day.

Recently, several banks around the world have failed to act on money laundering and have been fined millions. Several countries have failed to act on money laundering, and have lost millions in foreign direct investment.

Law enforcement agencies and the private sector in South Africa will have to start relying on using advanced accounting software to detect proceeds of crime and money laundering transactions if they are to comply with existing legislation and combat these types of crimes.

LIST OF REFERENCES

Babbie, E. 1998. *The practice of social research,* 8th edition. Belmont, CA: Wadsworth Publishing Company.

Bologna, J. 1995. *Fraud auditing and forensic accounting.* New York: John Wiley & Sons Inc.

Bortner, M. 1996. *Cyber laundering: Anonymous digital cash and money laundering* [online]. Available on the Internet at: http://www.osaka.law.miami.edu/~froomkin/seminar/papers/bortner.htm (accessed 23 April 2007).

Chester, T. 1994. *Mastering Excel 5 for Windows.* California: SYBEX.

Chinner, R. 2004. *Abdul Jabbar versus the National Director of Public Prosecutions (2003).* Johannesburg Asset Forfeiture Unit.

Cliffe, D. 2004. *Financial Services Authority – Royal Bank of Scotland fined £ 1,250 000 million* [online]. Available on the Internet at: http://www.fsa.gov.co.uk (accessed 16 February 2005).

Complinet. 2006. *Client screening, 2006 Enterprise Edition* [online]. Available on the Internet at: http://www.complinet.com (accessed 11 July 2006).

Currency and Exchanges Act *see* South Africa. 1933.

De Koker, L. 2003. *Money laundering in South Africa*. Pretoria: Mega Print CC.

Denscombe M. 2002. *Ground rules for good research: A 10 point guide for social researchers.* Philidelphia: Open University Press.

Excel. Microsoft Excel [computer program]. Windows. 2003. [s.l.]: Microsoft Corporation.

Financial Intelligence Centre of SA. 2004. *Authorized Officers Course Material.* Pretoria.

Fortent Ltd. 2005. *ABSA selects the Fortent Anti-Money Laundering Solution* [online]. Available on the Internet at: http://www.fortent.com (accessed 3 March 2006).

Fortent Ltd. 2006a. *Nedbank Ltd goes live with Fortent Anti-Money Laundering Solution* [online]. Available on the Internet at: http://fortent.com (accessed 11 July 2007).

Fortent Ltd. 2006b. *Largest South African bank goes live with Fortent's Anti-Money Laundering System* [online]. Available on the Internet at: http://fortent.com (accessed 11 July 2007).

Fox, W. 2004. *Riggs Bank fined US $ 25 million* [online]. Available on the Internet at: http://www.fincen.com (accessed 17 April 2007).

Fox, W. 2005a. *Arab Bank fines US $ 24 million* [online]. Available on the Internet at: http://www.fincen.com (accessed 17 April 2007).

Fox, W. 2005b. *ABN AMRO Bank fined US $ 80 million* [online]. Available on the Internet at: http://www.fincen.com (accessed 17 April 2007).

Goredema, C. 2003. *Profiling money laundering in eastern and southern Africa.* Pretoria: Mega Print CC.

Gormley, T. 2005. *ABN AMRO Bank fined $ 80 million* [online]. Available on the Internet at: http://www.fincen.gov/abnamro.html (accessed on 12 May 2006).

Hoogstrate, A.J., Van Den Heuvel, H. & Huyben, E. 2000. *Ear identification based on surveillance camera's Images* [online]. Available on the Internet at: http://www.forensic-evidence.com (accessed on 27 December 2007).

i2 Ltd. 2007. *i2 Analyst Notebook 7: i2 iBase 5* [online]. Available on the Internet at: http://www.i2.co.uk/Products/iBase/default.asp (accessed 10 August 2007).

Jost, P. & Sandhu, H.S. 2000. *The Hawala alternative remittance system and its role in money laundering* [online]. Available on the Internet at http://www.interpol.int/Public/Financial Crime/Money Laundering/hawala/default (accessed 15 December 2006).

KPMG. 2007. Global Anti Money Laundering Survey 2007 [online]. Available on the internet at http://www.kpmg.co.uk (accessed on 7 January 2008).

Lee, W. 2002. *Banks invest in new technology to target money laundering* [online]. Available on the Internet at http://www.searchspace.com/news/showMedia.php?id=28 (accessed 23 August 2005).

Leedy, P.D. & Ormrod, J.E. 2001. *Practical research: Planning and design.* 7th edition. Ohio: Merrill Prentice Hall.

Leedy, P.D. & Ormrod, J.E. 2005. *Practical research: Planning and design.* 8th edition. Ohio: Merrill Prentice Hall.

Leppan, D. 2005. *Helping define the PEP definition* [online]. Available on the Internet at: http://www.World-Check.com (accessed 26 November 2006).

Maimbo, S.M. 2003. *The money exchange dealers of Kabul: A study of hawala system in Afghanistan.* World Bank working paper no 13. Washington DC: The World Bank [online]. Available on the Internet at: http://www-wds.worldbank.org (accessed 10 January 2007).

Mantas Inc. 2003. *Using behavior detection to identify operational risk* [online]. Available on the Internet at: http://www.mantas.com (accessed 26 September 2007).

Mantas Inc. 2004. *Mantas Anti-Money Laundering solution overview* [online]. Available on the Internet at: http://www.mantas.com (accessed 26 Septemer 2007).

Marinos, G. 2005. *Data Management: An executive briefing: The quiet crisis in anti-money laundering strategies* [online]. Available on the Internet at: http::://www.dmreview.com. (accessed 26 April 2007).

McCusker, R. 2005. *Understanding underground banking: Legitimate remittance network or money laundering system?* [online]. Available on the Internet at: http://www.aic.gov.au/publications/tandi2/tandi300t.html (accessed 22 August 2005).

Michell, M. 2005. *Financial Intelligence Centre Annual Report 2004/2005* [online]. Available on the Internet at: http://www.treasury.gov.za (accessed 22 August 2007).

Michell, M. 2006. *Financial Intelligence Centre Annual Report 2005/2006* [online]. Available on the Internet at: http://www.treasury.gov.za (accessed 28 August 2007).

Microsoft Word [computer program]. . Microsoft XP Professional 2003. [s.l.]: Microsoft Corporation

Miller, R.L. & Brewer, J.D. 2003. *The A-Z of Social Research: A dictionary of Key Social Science Research Concepts* SAGE: London.

Mouton, J. 2001. *How to succeed in your Masters and Doctoral Studies*. *A South African guide and resource book*. Pretoria: Van Schaik.

OFAC Act *see* United States. 1990.

Passas, N. 2003. *Hawala and other Informal Value Transfer Systems: How to regulate them?* [online]. Available on the Internet at: http://www.usinfo.state.gov (accessed 13 March 2005).

POCA Act *see* South Africa. 1998.

POCDATARA Act *see* South Africa. 2004.

Roper, P. 2001. *Offshore Insight.* Johannesburg: Butterworths.

Sanjaya, R.M. 2005. *Understanding the role of technology in anti-money laundering compliance* [online]. Available on the Internet at: http://www.infosys.com (accessed 5 May 2007).

Searchspace Ltd. 2002. *Banks invest in new technology to target money laundering* [online]. Available on the Internet at: http:/www.searchspace.com/news/showMedia.php?id=28 (accessed 23 August 2005).

Searchspace Ltd. 2004a. *Meeting the regulatory challenge in South Africa* [online]. Available on the Internet at: http://www.searchspace.com (accessed 2 February 2006).

Searchspace Ltd. 2004b. *Using Searchspace for anti money laundering investigations. AML Sentinel for retail, corporate and private banking* [online]. Available on the Internet at: http://www.searchspace.com (accessed 2 February 2006).

Searchspace Ltd. 2006. *Fortent announced as new owner of Searchspace Ltd* [online]. Available on the Internet at

http://www.searchspace.com/news/showPress.php?id=96 (accessed 22 October 2007).

South Africa. 1933. Currency and Exchanges Act 9 of 1933. Pretoria: Government Printer.

South Africa. 1990. Banks Act 94 of 1990. Pretoria: Government Printer.

South Africa. 1998. Prevention of Organised Crime Act 121 of 1998. Pretoria: Government Printer.

South Africa. 2001. Financial Intelligence Centre Act 38 of 2001. Pretoria: Government Printer.

South Africa. 2004. Protection of the Constitution and Democracy and Terrorism and Related Activities Act 33 of 2004. Pretoria: Government Printer.

South Africa. South African Police Service. 2006. *Research in the Police Service, Circular, National Instruction 1/2006.* Commissioner of Police.

United States. 1990. Office of Foreign Assets Control regulations, United States. Washington D.C: Government Printer.

Welman, J.C. & Kruger, S.J. 1999. *Research methodology for the business and administrative sciences*. Johannesburg: Thompson.

Wikipedia. 2007. *Structuring/Smurfing (crime)* [online]. Available on the Internet at: http://www.wikipedia.org/wiki/Smurfing (crime) (accessed 13 August 2007).

INTERVIEWS

Respondent 4, Senior Technical Advisor Johannesburg Stock Exchange (JSE). 2007. 30 May. Sandton.

Respondent 6, Regional Compliance Officer, Moneygram International. 2007. 28 May. Sandton.

Respondent 9, Money Laundering Reporting Officer, Standard Bank Limited. 2007. 7 June 2007. Johannesburg.

Respondent 10, Consulting Chartered Accountant of South Africa (CASA). 2007. 2 June. Centurion.

Respondent 19, Detective/Captain Johannesburg, Commercial Crime Unit. 2007. 29 June. Johannesburg.

CASES

Abdul Jabbar versus the National Director of Public Prosecutions (2003).

Mohamed Suliman Vaid and Moshena Vaid versus the National Director of Public Prosecutions (2001).