Modelling of money laundering and terrorism financing typologies

Angela Samantha Maitland Irwin and Kim-Kwang Raymond Choo
Information Assurance Group and Forensic Computing Lab, University of South Australia, Adelaide, Australia, and

Lin Liu
School of Computer and Information Science, University of South Australia, Adelaide, Australia

Abstract

Purpose – The purpose of this paper is to show how modelling can be used to provide an easy-to-follow, visual representation of the important characteristics and aspects of money laundering behaviours extracted from real-world money laundering and terrorism financing typologies.

Design/methodology/approach – In total, 184 typologies were obtained from a number of anti-money laundering and counter-terrorism financing (AML/CTF) bodies to determine the common patterns and themes present in the cases involved. Financial flows, transactions and interactions between entities were extracted from each of the typologies and modelled using the Unified Modelling Language (UML) features within Microsoft Visio.

Findings – The paper demonstrates how complex transactional flows and interactions between the different entities involved in a money laundering and terrorism financing case can be shown in an easy-to-follow graphical representation, allowing practitioners to more easily and quickly extract the relevant information from the typology, as opposed to reading a full text-based description. In addition, these models make it easier to discover trends and patterns present within and across Types and allow money laundering and terrorism financing typologies to be updated and published to the wider international AML/CTF community, as and when new trends and behaviours become apparent.

Originality/value – A set of models have been produced that can be extended every time a new scenario, typology or Type arises. These models can be held in a central repository that can be added to and updated by AML/CTF practitioners and can be referred to by practitioners to help them identify whether the case that they are dealing with fits already predefined money laundering and terrorism financing behaviours, or whether a new behaviour has been discovered. These models may also be useful for the development of money laundering and terrorism financing detection tools and the training of new analysts or practitioners. The authors believe that their work goes some way to addressing the current lack of formal methods and techniques for identifying and developing uniform procedures for describing, classifying and sharing new money laundering and terrorism financing with the international AML/CTF community, as and when they happen, in a simple but effective manner.

Keywords Terrorism, Financing, Money laundering, Modelling, Knowledge management, Anti-money laundering/counter terrorism financing, Virtual environments, Entity relationship modelling, Collaborative information sharing

Paper type Research paper

Journal of Money Laundering Control
Vol. 15 No. 3, 2012
pp. 316-335
© Emerald Group Publishing Limited
1368-5201
DOI 10.1108/13685201211238061

1. Introduction

In the late 1990s, the chairman of the Organisation for Economic Co-operation and Development's Financial Action Task Force (FATF) Working Group on Statistics and Methods stated that there was a "need to estimate the size of money laundering and quantify its constituent parts". At least four areas were highlighted for further quantitative measures, including: understanding the magnitude of the crime, understanding the effectiveness of counter-money laundering efforts, understanding the macro-economic effects of money laundering and understanding money laundering (Walker, 1998).

Today there is an abundance of data on global trends in financial crime, money laundering and terrorism financing and much work has been done in an attempt to produce accurate estimates of money laundering and terrorism financing flows, however, although a number of largely varied estimates have been offered, none of them can be irrefutably proven. Also, the quantitative issues that have been raised by anti-money laundering and the fight against terrorism financing have yet to be definitively answered (Biagioli, 2008) and no broadly approved measurement methodology has yet been developed (Fleming, 2009).

Quantifying money laundering and terrorism financing is a very necessary and worthwhile exercise, however, identifying and developing uniform procedures and techniques for quickly and easily describing, classifying and sharing new money laundering and terrorism financing techniques and behaviours with the wider international AML/CTF community is equally, if not more important, especially when the platforms, techniques and methods employed by adversaries change rapidly and are becoming more complex (Nardo, 2006).

A number of programmes are already in existence for sharing information on money laundering and terrorism financing typologies. For example, annual typologies and case study reports are published by many AML/CTF agencies to assist reporting entities to meet their AML/CTF obligations. These reports contain details of sanitised, successfully detected money laundering and terrorism financing cases and provide a wealth of information on current threats and trends, techniques employed and, in many cases, the amount of funds involved. However, since these reports are published annually, a potential vacuum is created where new money laundering or terrorism financing schemes may go undetected until the next batch of typology reports is published. In addition, these typology reports only provide a limited snapshot of some of the types of money laundering and terrorism financing activity detected in individual jurisdictions in that year and often only include cases where large sums of money have been detected, thereby potentially omitting a number of significant or new money laundering and terrorism financing behaviours or techniques. The format that the typology reports take can also pose problems due to their over-descriptive and case-specific nature.

What is required is a collaborative, synergistic reporting system that can be updated in real-time; thereby informing AML/CTF experts and investigators immediately or soon after a new technique or method has been discovered.

This view is supported by a number of authors who believe that high-level collaboration (Liu and Zhang, 2007), synergistic information sharing and knowledge management (Biagioli, 2006; Biagioli and Nardo, 2007; Global Justice Information Sharing Initiative, 2006; Hardouin, 2009; Mueller, 2006; O'Connell, 2008) are important aspects of a successful AML/CTF system.

Much can be learned through the exchange of non-classified data and increased levels of communication and exchange of ideas between intelligence and law enforcement agencies, financial investigation units, researchers and the private sector at national and international levels as these have proven to produce good results in the past (Hardouin, 2009).

An example of where a cooperative relationship paradigm has been successfully utilised is the "Spotlight" Project, a joint research project between Italy's Ufficio Italiano dei Cambio (UIC) and the London School of Economics (LSE) aegis of EC AGIS Program. The project relies on UIC methodological advice, the LSE's scientific direction and the expertise of a consortium of partners (including financial institutions, regulators and law enforcement agencies). The purpose of the project is to develop a methodology for creating effective money laundering monitoring tools. In line with its research objective, a holistic framework is proposed, so as to benefit from contributions coming from a wide range of quantitative, social and human disciplines (Biagioli, 2006).

Spotlight attempts to combine a profiling methodology with a behaviour-led approach to modelling, as well as defining the modelling approach in a way that makes it usable in other national and regulatory contexts. Their ambition is to build a tool that, through some proper customisation procedures, can be exported to wider and different environments.

Biagioli and Nardo (2007) discuss the importance of collaboration and the sharing of information and competencies between bankers, lawyers, law enforcement officers and economists. They believe that the present professions might be stretched towards a new level of specialisation that may allow them to carry out osmotic flows of information through those contact lines and areas that, until now, have represented a restraining element and a potential obstacle. The authors imagined the dissolution of barriers that following a path of integration leading to a merging into one single unit, the excellent elements that have characterised each individual profession thus far. "Bridging the frontier" would mean, however, investing in education, building an area of shared information and knowledge, conceiving a unified territory, not just a common platform, where all potentialities deriving from the different disciplines, institutions and experiences might converge. In the views of the authors, this has become an operational need and, given the present institutional and regulatory framework, they believe that a critical mass has been reached.

Biagioli (2006) also looked at the evolution of organisational science in the application of knowledge sharing and knowledge management. He believed that it was necessary to proceed along the steps of enhancing knowledge capital to generate a knowledge base, identifying strategies of knowledge management and showing the costs and benefits in terms of content and procedures to generate a culture of knowledge management whereby a consensus for change could be reached.

Like Hardouin (2009) and Biagioli (2006) subscribed to the view that know-how should be derived from different sources, fields and experiences. However, he argues that a mere "paper-pushing" attitude should not be adopted; rather, it requires the proper management of different pieces of information to be used to build knowledge; a management strategy which goes far beyond the sharing of documents and news. The process Biagioli (2006) has in mind is quite unlike the concept of benchmarking, where one tries to adjust his actions to a declared objective: what one should aim for is the definition of a new paradigm; a (yet unknown) principle based on rules of integration and unified vision.

Therefore, synergy is essential for successful knowledge management and information sharing as every actor's skills and knowledge is precious and may prove vital to anti-money laundering and terrorism financing detection.

Better understanding of the current threat landscape (including current and emerging money laundering and terrorism financing schemes) allows us to model, simulate and forecast criminal action more accurately and intervene more effectively to prevent it. By collecting and crossing information from different aspects and approaches, information is transformed into systematic knowledge which, in turn, can be used to develop further information (Biagioli, 2006).

A number of authors have highlighted behaviour modelling as a vital component in a successful AML/CTF system (Biagioli, 2006; Biagioli and Nardo, 2007; Gao *et al.*, 2009; Nardo, 2006). However, representing human behaviour can be a very difficult and complex task. Before attempting to represent the human behaviour resident in any domain, much thought must be given to how to frame the problem. More specifically, one can view the ultimate representation as a set of people, functional behaviours, and processes, or one may choose to view the representation as a set of flows and controls. Each framework gives rise to unique modelling considerations and requirements (Wise *et al.*, 2001).

Modelling helps us to develop a better understanding of complex environments. The greater the level of uncertainty that surrounds an environment, the more valuable modelling becomes.

The reason for modelling the environment dictates the type of tool(s) used. For example, is the purpose to communicate a set of behaviours or sequence of steps to a third party or is it to perform an in-depth analysis and verification of patterns identified.

The whole process of model building balances on the appropriate design of the path that goes from choosing the elements to describe the behaviour, to identifying the most accurate parameters to reflect them, and finally to defining proper queries that match parameters within the available data. Good design is logically and rationally grounded, reasonable in its basis as well as in its development, and sheltered from the risks coming from unsound basic assumptions, erroneous process or distortions, which can hamper the path and produce unreliable results. To this end, a proper methodology must assist and assess every one of the several components and steps of the modelling process. In addition, methodology must assist properly the correct implementation of each phase (Nardo, 2006).

Alach (2010) constructs a model of the "methamphetamine ecosystem" from a law enforcement perspective. Although much was already known on the subject of methamphetamines, most of the information was held in separate silos and had not been analysed in context. The first stage of the author's approach involved identifying high-level processes within the ecosystem, identifying the interactions between those processes and specific actors, analysing workflows within the ecosystem, enriching information held on specific behaviours, and combining all of this information into a dynamic model. By visualising the methamphetamine problem as a system of systems, the author was able to identify new vulnerabilities and establish better metrics for establishing success.

Similar to AML/CTF, the methamphetamine ecosystem is a complex one. By "modelling the enemy as a system", Alach (2010) was able to create a complex, holistic model which could be built up over time and create a powerful tool for targeting drug control decisions.

Nardo (2004) investigates mapping the trails of financial crime. He argues that it is necessary to know more about the movements that go through the markets:

the causes, options, instruments available and opportunities that arise from all of these in order to allow us to intervene better and more rapidly to financial crime. Nardo believes that the modelling approach provides a powerful conceptual tool at both fact-finding and problem-solving levels by facilitating the gathering and selection of vast quantities of data and permitting the organisation of knowledge into synthetic forms and increasing understanding, schematisation, creation of logical linkups, linear construction of hypotheses through identifying and evaluating more clearly interpretations, opinions, ideas and various solutions to problems.

Although little can be found which relates to modelling specific behaviours and the sequence of steps and interactions that may be associated with money laundering and terrorism financing activity, it is clear that modelling has provided many benefits for other highly complex, data rich environments.

Modelling provides us with enriched information, thereby furnishing us with a greater understanding and knowledge of the threat landscape. This increase in understanding allows us to better target overstretched human and financial resources and tighten up or close some of the gaps which enable money launderers and terrorism financers to carry out their activities unimpeded.

2. Focus of research

Our three-year research project, which primarily aims to determine whether it is possible to launder money and raise funds for terrorism inside virtual environments such as Second Life and World of Warcraft, is split into six distinct phases (Figure 1).

Phase 1 of research was completed earlier this year and involved the collection and statistical analysis of 300 money laundering and terrorism financing typologies (Anonymous, forthcoming). The statistical analysis phase attempted to measure the size of the money laundering and terrorism financing problem, identify threats and trends, the techniques employed and the amount of funds involved to determine whether the information obtained about money laundering and terrorism financing in real-world environments could be transferred to virtual environments such as Second Life and

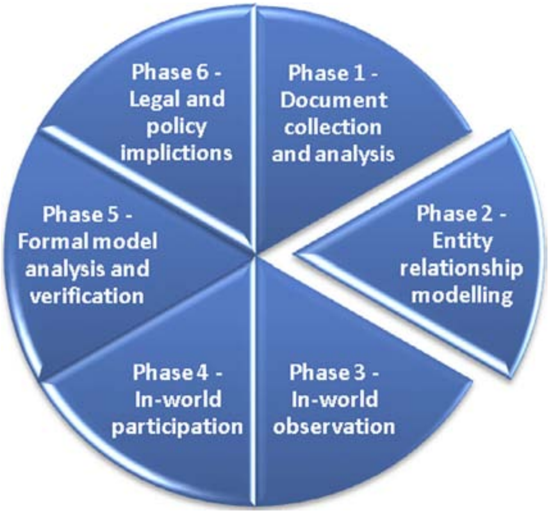

Phase 6 - Legal and policy implictions
Phase 1 - Document collection and analysis
Phase 2 - Entity relationship modelling
Phase 3 - In-world observation
Phase 4 - In-world participation
Phase 5 - Formal model analysis and verification

Figure 1.
Phases of research

World of Warcraft. Findings from Phase 1 indicated that money launderers and terrorism financers may have slightly different preferences for the placement, layering and integration techniques. The more techniques that were used, the more cash could be successfully laundered or concealed. Although terrorism financers used similar channels as money launderers, they did not utilise as many of the placement, layering and integration techniques available. Rather, they preferred to use a few techniques which maintained high levels of anonymity and appeared innocuous. The sums of monies involved in money laundering and terrorism financing varied significantly. For example, the average maximum sum involved in money laundering cases was AUD 68.5M, compared to AUD 4.8M for terrorism financing cases.

This paper discusses Phase 2 of research, which shows how modelling can be used to provide an easy-to-follow, visual representation of the important characteristics and aspects of money laundering and terrorism financing behaviours which have been extracted from the real-world money laundering and terrorism financing typologies collected at Phase 1 of research. These models will be used as a starting point for determining whether each typology can be carried out inside Second Life or World of Warcraft in Phase 3. UML will be used in Phase 2 to produce an easy-to-follow, visual illustration of the behaviours, transactions and interactions between each of the actors in the money laundering and terrorism financing typologies. UML allows us to create meaningful models which show a holistic view of the whole ecosystem under investigation. The extensible nature of UML means that the models created can be continually enhanced and updated whilst at the same time only contain the pertinent details of the money laundering and terrorism financing system that are required to understand it.

During Phase 3, it will also be established whether there are any additional money laundering and terrorism financing Types that have not been uncovered during analysis of the real-world money laundering and terrorism financing typologies because they are unique to Second Life and World of Warcraft.

During Phase 4, the in-world participation phase, there will be an attempt to replicate the typologies deemed as possible in virtual environments. This will be done by creating the conditions necessary to carry out the behaviours and patterns identified for each Type. For example, we will create the individuals (avatars) and/or entities (businesses) that will be required to carry out the money laundering/terrorism financing transaction(s). We will then try to replicate the interactions, financial or otherwise, that would need to take place between the individuals and/or entities for a successful transaction to take place.

Phase 5, formal analysis and verification, will be conducted to provide a scientific and measurable approach to the research. All of the money laundering and terrorism financing Types that are successfully replicated inside Second Life and World of Warcraft will be modelled and analysed using formal methods, such as coloured Petri nets (University of Aarhus, 2011), which have been used successfully to verify human behavioural patterns in virtual environments (Köhler *et al.*, 2001; Piccard, 2008; Chang *et al.*, 2009) and script the complex behavioural sequences of virtual actors within virtual environments (Blackwell *et al.*, 2001). A set of models, similar to those created in Phase 2 will also be constructed with the view that they can be used in any information sharing, collaboration efforts.

The final phase of research investigates the legal environment for the detection and prosecution of money laundering and terrorism financing in virtual environments, such as Second Life and World of Warcraft, and discusses the implications this might have on government policy.

This paper demonstrates how complex transactional flows and interactions between the different entities involved in a money laundering and terrorism financing case can be shown in an easy-to-follow, graphical representation, allowing readers to more easily and quickly extract the relevant information from the typology as opposed to reading a full text-based description. In addition, these models make it easier to discover trends and patterns present within and across Types[1] and allow money laundering and terrorism financing typologies to be updated and published to the wider international AML/CTF community as and when new trends and behaviours become apparent.

The rest of the paper is structured as follows: Section 3 provides a general background to money laundering and terrorism financing activity; Section 4 discusses the methodological approach used for modelling the money laundering and terrorism financing typologies; and Section 5 provides examples of modelled money laundering behaviour. Finally, the last section concludes the paper.

3. Background

Although there are many definitions for money laundering, depending on whether you are looking at it from a legal, economic or social perspective, the definition applied to this project is the one used by the Australian Institute of Criminology which states that:

> [. . .] money laundering is the process by which the proceeds of crime are put through a series of transactions, which disguise their illicit origins, and make them appear to have come from a legitimate source (Graycar and Grabosky, 1996).

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention (FSC, 2009).

There are three phases to money laundering; placement, layering and integration (FATF-GAFI.org, 2011). In the placement stage, the cash generated from crime is brought into the financial system. At this point the proceeds of crime are most apparent and at highest risk of detection. Money launderers "place" the illegal funds using a variety of techniques, which include the deposit of cash into bank accounts and the use of cash to purchase high value assets such as land, property and luxury items. Once the proceeds of crime have been placed into the financial system, there is an attempt to conceal or disguise the source or ownership of the funds by creating complex layers of financial transactions. The purpose of this is to disassociate the illegal monies from the source of the crime by purposefully creating a complex web of financial transactions aimed at concealing any audit trail and the source and ownership of funds. The final stage in the process is where the money is integrated into the legitimate economic and financial system and is absorbed with all other assets in the system. Integration of the cleaned money into the economy is accomplished by the launderer making it appear to have been legally earned. It is extremely difficult to discern between legal and illegal wealth at the integration stage.

Terrorism financing, on the other hand, occurs when the primary motivation is not financial gain but, rather, the use of funds to "encourage, plan, assist or engage in" acts of terrorism (WorldBank.org, 2003). Funds are often transferred using tactics that are progressively more complex. Terrorist financing networks operate globally and are able to gain access to the financial systems of both developing and developed countries.

The terrorism financing model differs from the money laundering model in that terrorism financing funds can be from legitimate sources, not just criminal acts, as is the case with money laundering. For example, significant funds can be raised through legitimate businesses, fund raising efforts and donations.

Although there can be a number of different motivators and drivers for money laundering and terrorism financing activity, they are inextricably linked. Terrorist groups usually have non-financial goals: publicity, dissemination of an ideology, the destruction of a society or regime, and simply spreading terror and intimidation. However, in practice, terrorists need finances and are often profit-oriented groups in addition to their ideological motivations (Hardouin, 2009).

It must be noted that money laundering and terrorism financing do not necessarily go hand-in-hand as a great deal of money laundering activity is for private profiteering only and not for political purpose (Choo and Smith, 2008).

4. Methodology

In order to answer the main research question, "Can money laundering and terrorism financing occur in virtual environments?" one must know what money laundering and terrorism financing in these environments might look like. Since this information does not currently exist, we look to data published by a number of AML/CTF bodies to inform our research. The advantage of using this data is that it resembles and represents underlying money laundering and terrorism financing trends; it contributes to an understanding of the scale and nature of predicate offences and, due to standardised reporting procedures, it provides relevant, time-specific data that can be easily collected.

About 300 typologies, with dates ranging from 1996 to 2009, were obtained from a number of AML/CTF bodies, namely, AUSTRAC, the Egmont Group, FATF, the Belgian Financial Intelligence Unit (CTIF-CFI) and Moneyval. Typologies were collected from a number of international jurisdictions in order to gain a wide spread of money laundering and terrorism financing methods and behaviours.

The typologies were grouped into Types to ease analysis and assist us in determining the common patterns and themes present in the cases involved. Typologies that had commonality in the type(s) of predicate offence[2] were grouped together. In Australia, money laundering offences are criminalised at both Commonwealth and state and territory levels. The definition of money laundering at the Commonwealth level is given in Division 400 of the Criminal Code Act 1995 (Cth). The Commonwealth Act does not limit predicate offences with a specific list. Predicate offences are, instead, those with a minimum sentence of at least one year's imprisonment. The offences at a state and territory level differ according to areas such as relevant predicate offences, the intent of the defendant, and penalties attached to the offences. Some difficulty was experienced in classifying the terrorism financing typologies as a predicate offence was not always present or reported. However, it is important to note that in its Second Special Recommendation on Terrorist Financing (FATF-GAFI.org, 2004), FATF recommended that terrorism financing be listed as one of the predicate offences to money laundering. Nevertheless, using this approach adds little value to the analysis process, therefore, where a specific predicate offence is not indicated, the technique used to conceal the funds is used to classify the typology.

Although 300 typologies were collected, 116 of them were considered unsuitable for analysis and modelling as they contained a large degree of ambiguity or did not contain enough information on financial flows, transactions or interactions between entities to provide value to the research. This number was reduced further when the typologies were analysed to determine their uniqueness. For example, if five typologies in a Type had a large degree of correlation, the typologies were analysed and modelled only once but contained all of the pertinent information, extracted from each of the typologies. In addition, some of the typologies could be classified under more than one category as they incorporated a number of predicate offences. When this occurred, the typology was classified under the primary predicate offence that took place and modelled only once.

Table I shows how the typologies were classified and the number of typologies that were subsequently utilised in the research.

Each of the typologies were examined in fine detail to gain a better understanding of the motivations, the wide range of techniques employed by individuals and entities and the levels that individuals and organisations would go to in an effort to hide their illegal or illicit activity. The following key information was extracted from each of the typologies:

- The individuals and/or entities involved in the ML/TF scheme.
- The type of transaction(s) involved in the ML/TF scheme. For example, cash, cheque or electronic funds transfer.
- The interactions, financial and otherwise, that took place between the individuals and entities involved in the ML/TF scheme.
- The suspicious behaviours and red flag indicators detected by the reporting entity.

Table I.
Classification of typologies collected and modelled

Money laundering	Terrorism financing
Primary predicate offence	Primary predicate offence or technique employed
Corruption (4)	Collection of donations (4)
Fraud[a] (56)	Use of unlicensed money transmitters/remittance agents[b] (3)
Gambling (2)	Purchase of high value assets[c] (3)
Sex trade (1)	Intimidation and extortion (1)
Trafficking	Trafficking
Commodity[d] (14)	Human (1)
Human (8)	Diamond (1)
Drug (40)	Counterfeit goods (1)
Tax evasion (13)	Tax evasion (2)
Theft (7)	Use of not for profit organisations (12)
	Purchase of cheques or money orders (2)
	Use of front companies (2)
	Early cancellation of insurance policies (2)
	Concealment within business structures (4)

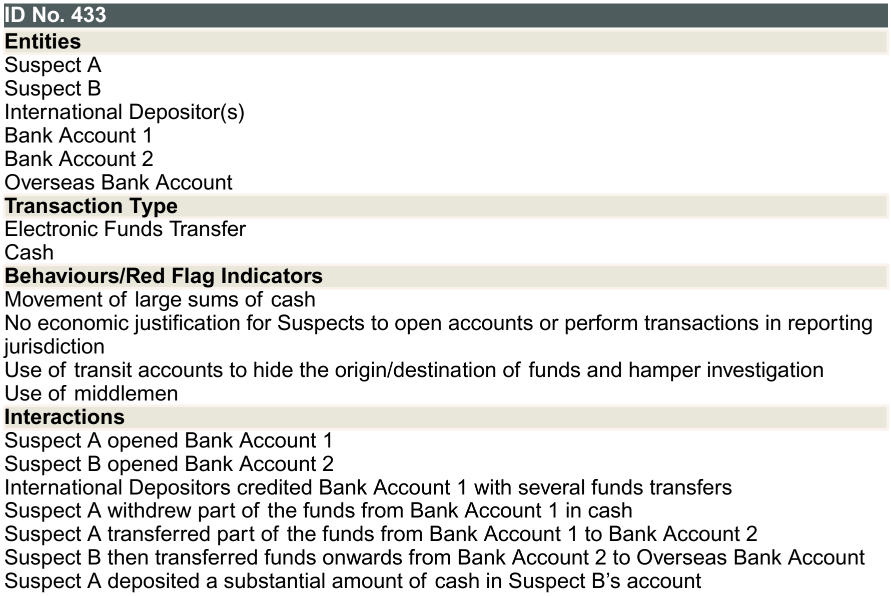
Notes: [a]Fraud includes corporate, investment scheme and bankruptcy fraud; [b]this includes the predicate offence of a business or individual operating as unlicensed money transmitters/remittance agents to facilitate the movement of funds to terrorist organisations; it also includes individuals who use unlicensed money transmitters/remittance agents to send funds to a terrorist organisation; [c]this refers to the purchase of high value assets, such as property, to conceal funds raised for terrorism financing; these funds may be from legal (such as fund raising) or illegal (such as the proceeds of criminal activity) means; [d]commodity trafficking includes arms, gold, counterfeit cheques and designer items, illegal hormones, diamonds, stolen vehicles and cigarettes and alcohol smuggling

An example of a typical money laundering or terrorism financing typology is shown below:

> A and B, who resided abroad, had opened an account on which suspicious transactions took place. A's account was credited by several international transfers from offshore centre X. Part of the funds was withdrawn in cash, another was transferred to B's account and finally transferred to an account B held abroad. In addition A had deposited a substantial amount in cash on B's account. To justify the origin of these funds he showed the statement of the withdrawal from the account opened in offshore centre Y. He announced that an even higher amount would be transferred shortly. There was no economic justification for A and B to open an account and to perform transactions in Belgium, which indicated that these accounts were used as transit accounts in order to hamper possible investigation into the origin and/or the destination of the money. Information obtained from the unit in A's country of residence showed that A and B were the subject of a money laundering investigation. In addition, it became clear that A was linked to the former president of an African country. The latter had embezzled significant amounts of money to the detriment of his country when he was in power. An important part of the government money was placed on accounts in offshore centre X. Furthermore, the international transfers crediting A's accounts were also from offshore centre X. The African country in question had also requested legal assistance from the country in which A resided and from offshore centre Y. Based on all of these elements, it could be deduced that the financial transactions performed by A and B in Belgium appeared to be linked to the former African president's illegal activities. The case file was transmitted with regard to corruption. A police investigation is underway. This case files illustrates the international dimension of money laundering. Individuals, who are not linked to Belgium in any way, frequently open accounts with financial institutions in our country just for performing money-laundering transactions. It also illustrates that politically exposed persons (PEPs) often have middlemen perform money laundering transactions on their behalf to avoid unwanted questions on their activities. Finally, this once again emphasizes the importance of good international cooperation with foreign counterpart units (Belgian Financial Intelligence Processing Unit, 2005).

To ease the modelling process, a template form was created to collect all of the relevant data on behaviours, transactions and interactions. Wherever possible, typologies were combined to avoid duplication of information collected. For example, if a number of typologies, which were related to a specific Type, had high degrees of similarity they would be included on one template form. Figure 2 shows an example of how the template form was used to extract the relevant information from the typology depicted in the quote (an example of a typical money laundering typology) above.

Once the relevant information was extracted from the typology, the information was modelled using the UML model features within Microsoft Visio. Microsoft Visio was used because it is a general-purpose, ready-to-use and expressive visual modelling tool that can be used to specify, visualise, construct and document a wide variety of systems. The benefit of Visio is that the interface is quite intuitive and there are general drawing tools that help users to customise diagrams/models to their own specific needs. Although Microsoft Visio provides separate use case, structure, behaviour and interaction diagrams, we used only the use case diagram to model the typologies as we felt that it was more important for our project to have all of the information related to a typology on the one model. However, if a collaborative information sharing, knowledge management system was to be put in place, the structure, behaviour and interaction diagrams could be utilised by practitioners as this would enable the models created to be easily slotted into future AML/CTF tools. Figure 3 shows an example of a Visio Use Case diagram created from the data collected in the money laundering related to corruption typology shown in Figure 2.



ID No. 433

Entities

Suspect A
Suspect B
International Depositor(s)
Bank Account 1
Bank Account 2
Overseas Bank Account

Transaction Type

Electronic Funds Transfer
Cash

Behaviours/Red Flag Indicators

Movement of large sums of cash
No economic justification for Suspects to open accounts or perform transactions in reporting jurisdiction
Use of transit accounts to hide the origin/destination of funds and hamper investigation
Use of middlemen

Interactions

Suspect A opened Bank Account 1
Suspect B opened Bank Account 2
International Depositors credited Bank Account 1 with several funds transfers
Suspect A withdrew part of the funds from Bank Account 1 in cash
Suspect A transferred part of the funds from Bank Account 1 to Bank Account 2
Suspect B then transferred funds onwards from Bank Account 2 to Overseas Bank Account
Suspect A deposited a substantial amount of cash in Suspect B's account

Figure 2.
Example of use of form to collect data on money laundering related to corruption

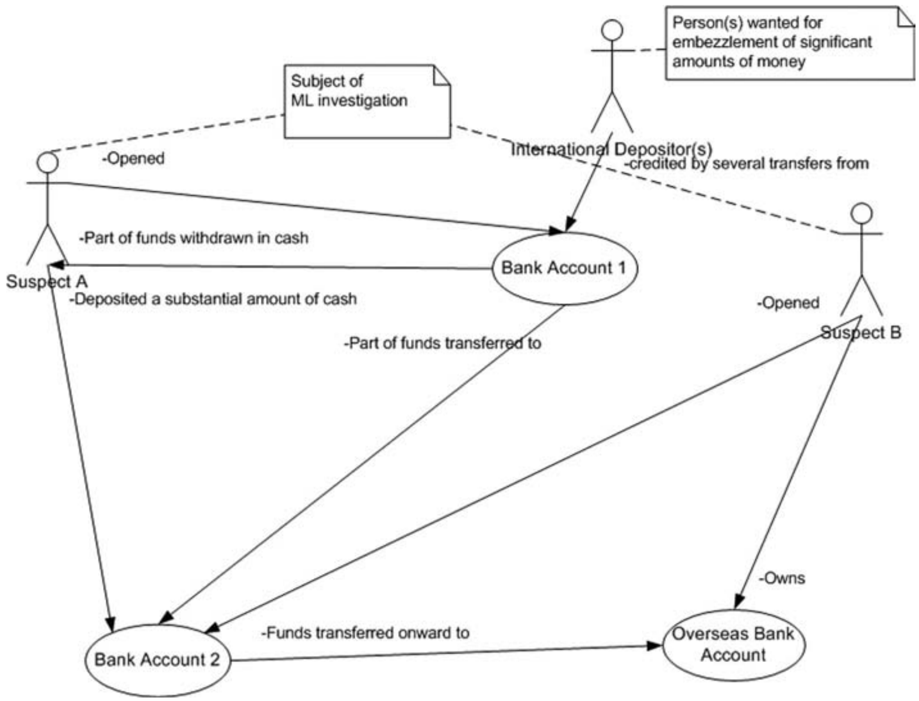

Person(s) wanted for embezzlement of significant amounts of money
Subject of ML investigation
International Depositor(s)
-credited by several transfers from
-Opened
Suspect A
-Part of funds withdrawn in cash
Bank Account 1
-Deposited a substantial amount of cash
-Opened
Suspect B
-Part of funds transferred to
-Owns
-Funds transferred onward to
Bank Account 2
Overseas Bank Account

Figure 3.
Model created from the data collected in the money laundering related to corruption typology shown in Figure 2

Wherever possible, additional information was added to the model to help the reader understand the finer details of the money laundering or terrorism financing scheme which might not be evident from viewing the model alone. Comparing the quote (an example of a typical money laundering typology), an example of a typical money laundering typology and Figure 3, the model created from the data collected in the money laundering case related to the corruption typology, the model is far easier to follow and can be easily updated should new behaviours, entities or transaction types be discovered. In addition, as the old adage goes "a picture says a thousand words", this is vitally important in situations where a large number of native languages need to be considered. Since language-barriers may play a major role in whether or not information sharing and collaboration is successful, models offer the advantage that they are simpler to translate than text-only based descriptions, due to the small amount of language-specific text used.

5. Examples of modelled typologies

This section takes one of the money laundering Types, commodity trafficking, and shows how modelling can be used to represent the important characteristics and aspects of the money laundering behaviours discovered. Commodities, in the context of this project, includes stolen vehicles, contraband alcohol and cigarettes, counterfeit cheques and designer items, illegal hormones, diamonds, gold bullion and arms. Commodity trafficking allows businesses and individuals to avoid the significant amount of taxes that would be due if the goods were imported legally.

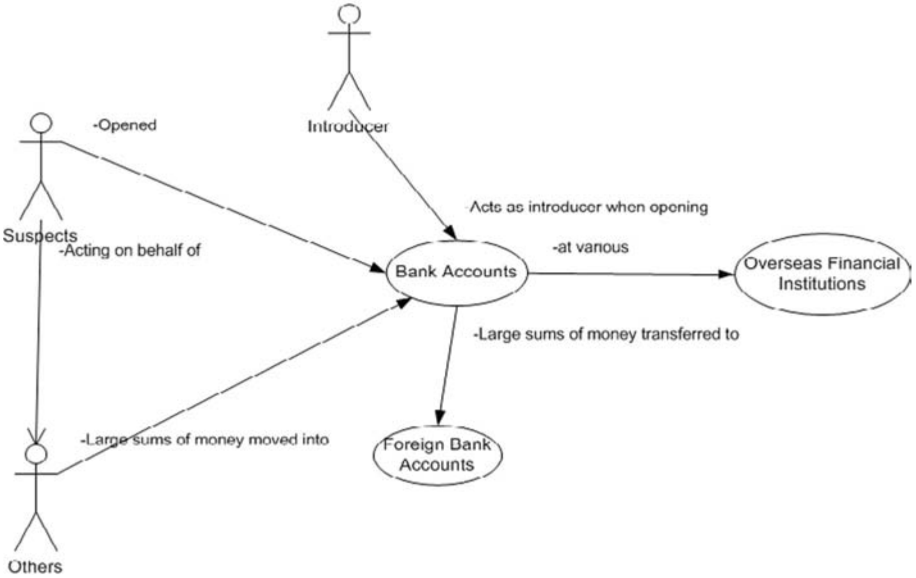
In the commodity trafficking scenarios studied, two clear trends could be identified, namely, the use of front men, front companies or shell companies to enter (or receive) illegal funds into the financial system (Figures 4-6), thereby, concealing or disguising the source and ownership of illegal funds and investing in securities and financial instruments (Figures 7-9) to integrate the funds into the legitimate economic and financial system to make the monies appear as though they were legally earned.

Figure 4 shows how the suspects in this scenario act as straw men for individuals who wish to remain anonymous and disassociated from the crimes that have taken place. The straw men open bank accounts in their own names or in the names of the companies that they own at various overseas financial institutions. These accounts are deposited with large amounts of illegal funds, which are then transferred onwards to other foreign bank accounts.

Figure 5 shows how front businesses were used to open bank accounts into which large sums of illegal funds were regularly deposited. Once the funds were deposited into the front company bank accounts, the funds were immediately transferred to an overseas bank account, opened by another front company.

Figure 6 shows how legitimate businesses and businesses set up solely to facilitate money laundering can collaborate to enter illegal monies into the legitimate economic and financial system. In this scenario, there is co-operation between a terrorist organisation and an organised criminal organisation to create a bureau de change solely to facilitate the laundering of smuggled proceeds. The contraband items are smuggled into the reporting jurisdiction using various methods. Once the contraband has been sold, the funds are transported to another jurisdiction using a cash courier. The funds are entered into the accounts of front/shell companies and then distributed to legitimate businesses, intermingled with their normal receipts.

Concealing smuggling activity within business structures disguises criminal funds within the normal activity of existing businesses controlled by the criminal organisation.


Introducer
Suspects
-Opened
-Acting on behalf of
Acts as introducer when opening
-at various
Bank Accounts
Overseas Financial Institutions
-Large sums of money transferred to
-Large sums of money moved into
Foreign Bank Accounts
Others

Interactions that took place were as follows:

1. ***Suspects**, acting on behalf of **Others'**, opened Bank Accounts at various **Overseas Financial Institutions***
2. ***Introducer** acts as introducer at the bank when **Suspects** opened Bank Accounts*
3. ***Others** deposited large sums of cash into Bank Accounts*
4. ***Suspects** transferred large sums of money from Bank Accounts to other Foreign Bank Accounts*

Red flag indicators present in this case :

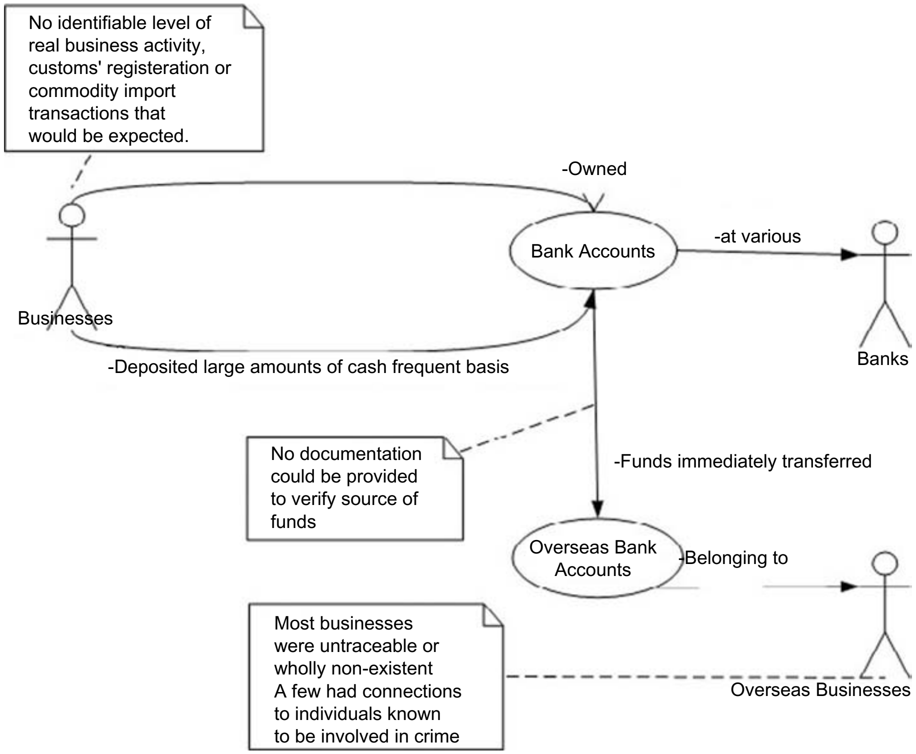
- *Lack of underlying business rationale for business activity*

  Multiple repeat movements of funds between accounts
- *An attempt to conceal the origin of funds/use of layering techniques*
- *Suspects under investigation for criminal activities*
- *Use of "straw men"*

Figure 4.
Use of straw men in commodity trafficking

Attempting to move funds through the financial system by intermingling them with the transactions of a controlled existing business has several advantages, namely: the criminal has more control over the company being used, either by beneficial ownership or a close relationship with the actual owner, which decreases the risk of being caught and the financial institution through which funds are passed may view fluxes in account activity with less suspicion than similar activity on a personal account.

Figures 7-9 show how suspects attempted to launder money through the investment of monies in a mortgage loan (Figure 7), the purchase of securities (Figures 8 and 9) and the purchase of life insurance policies (Figure 8). Investing in securities and financial instruments integrate funds into the legitimate economic and financial system to make the monies appear as though they were legally earned.


No identifiable level of real business activity, customs' registeration or commodity import transactions that would be expected.
-Owned
Bank Accounts
-at various
Businesses
Banks
-Deposited large amounts of cash frequent basis
No documentation could be provided to verify source of funds
-Funds immediately transferred
Overseas Bank Accounts
-Belonging to
Most businesses were untraceable or wholly non-existent A few had connections to individuals known to be involved in crime
Overseas Businesses

Interactions that took place were as follows:

1. ***(Front) Businesses*** *owned Bank Accounts at various* ***Banks***
2. ***(Front) Businesses*** *deposited large amounts of cash into the Bank Accounts on a frequent basis.*
3. *These funds were then immediately transferred from the Bank Accounts to a number of Overseas Bank Accounts owned by a number of* ***Overseas Businesses*** *(the true beneficial owners of the funds)*

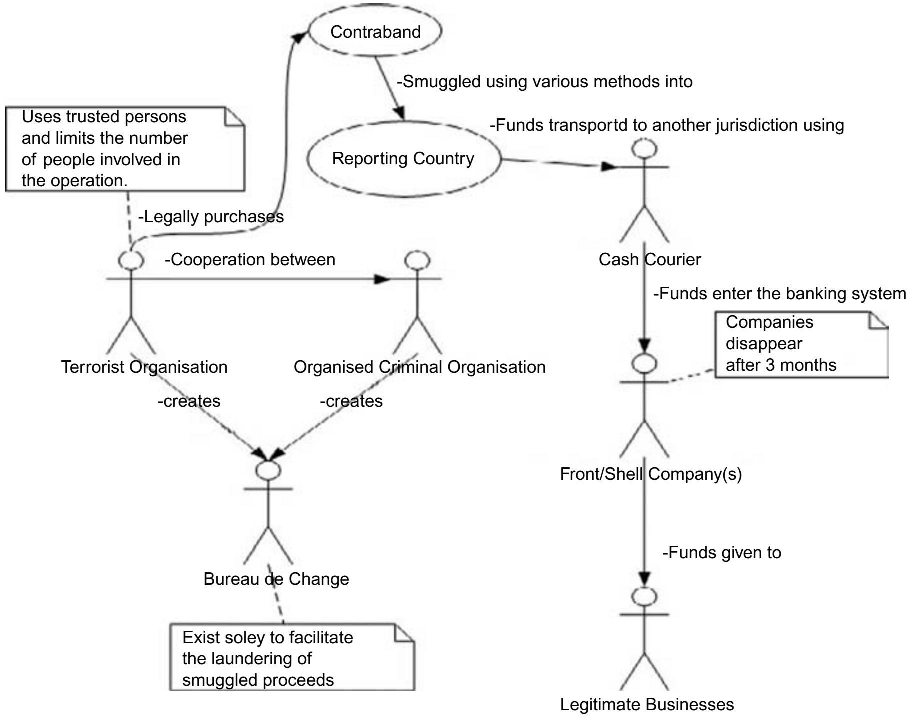
Red flag indicators present in this case:

- *No identifiable level of real business activity*
- *Multiple repeat movements of funds between accounts*
- *An attempt to conceal the origin of funds/use of layering techniques*
- *Source of funds could not be verified*
- *Use of "front companies" – companies were untraceable or non-existent*
- *Individuals known to be involved in criminal activity*

Figure 5.
Use of local and international front companies in commodity trafficking

It is expected that, at some time in the future, the suspect will prematurely terminate the insurance policies and be refunded a proportion of the funds paid into the policy, in so doing the monies will look as though they have been legally obtained.

When viewing the models collectively, trends and patterns present within and across Types can be identified. For example, analysis of each of the commodity trafficking cases


Contraband
-Smuggled using various methods into
Reporting Country
-Funds transportd to another jurisdiction using
Uses trusted persons and limits the number of people involved in the operation.
-Legally purchases
-Cooperation between
Cash Courier
-Funds enter the banking system
Companies disappear after 3 months
Terrorist Organisation
Organised Criminal Organisation
-creates
-creates
Front/Shell Company(s)
Bureau de Change
-Funds given to
Exist soley to facilitate the laundering of smuggled proceeds
Legitimate Businesses

Interactions that took place were as follows:

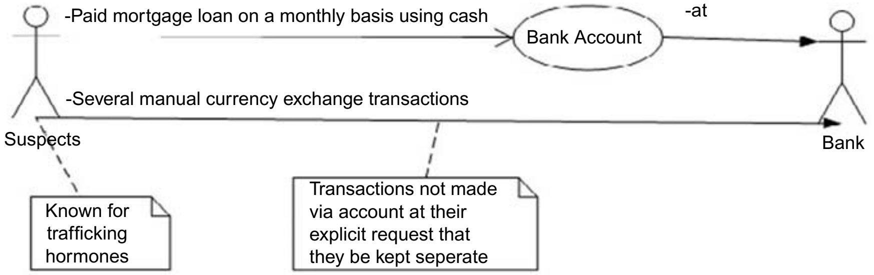
1. ***Terrorist Organisation*** *and* ***Organised Crime Organisation*** *cooperate to legally purchase Contraband.*
2. *Contraband is smuggled into Reporting Country using various methods.*
3. *Once inside Reporting Country,* ***Cash Courier*** *enters the funds into the banking system.*
4. ***Cash Courier*** *forwards funds to* ***Front/Shell Company(s)***
5. ***Front/Shell Company(s)*** *give funds to* ***Legitimate Businesses****. The funds enter the banking system as part of the* ***Front/Shell Company(s)*** *normal receipts.*
6. ***Terrorist Organisation*** *and* ***Organised Criminal Organisation*** *create* ***Bureau De Change*** *solely to launder smuggled proceeds.*

Red flag indicators present in this case :

- *Cash couriered to another jurisdiction*
- *Use of front companies or short-term shell companies*
- *Use of legitimate businesses*
- *Money passed through NCCTs*

Figure 6.
Use of legitimate and front companies in commodity trafficking

revealed that at least one of the entities involved in the money laundering scheme were known to police, had previous criminal convictions or were under active investigation for suspected criminal activities. An advantage of presenting money laundering and terrorism financing typologies in this way is that reporting of the behaviours,


-Paid mortgage loan on a monthly basis using cash
Bank Account
-at
-Several manual currency exchange transactions
Suspects
Bank
Known for trafficking hormones
Transactions not made via account at their explicit request that they be kept seperate

Interactions that took place were as follows:

1. *On a monthly basis,* ***Suspects*** *made cash payments to a Bank Account at* ***Bank*** *to pay mortgage*
2. ***Suspects*** *made manual currency exchange transactions at* ***Bank*** *but did not use Bank Account.*

Red flag indicators present in this case :

- *Mortgage loan paid exclusively by cash payments*
- *Requested financial activity be performed separately from bank account*
- *Known to have connections with criminal activity*

Figure 7.
Investment in mortgage loans to conceal commodity trafficking

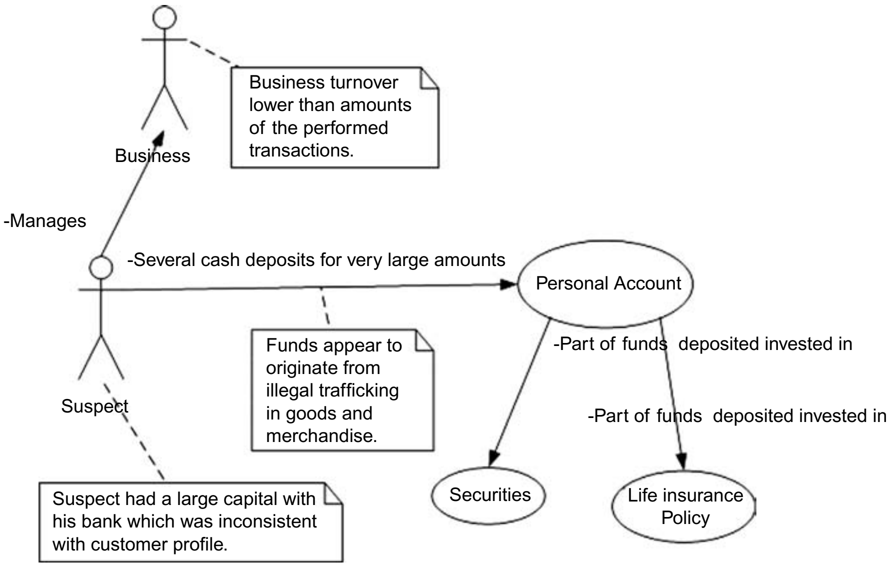
trends and patterns can be described in a consistent and very reader-friendly manner as there is no need for lengthy and wordy descriptions.

6. Conclusion

There is, arguably, a great need for the identification and development of uniform procedures and techniques for quickly and easily describing, classifying and sharing new money laundering and terrorism financing techniques and behaviours with the wider international AML/CTF community in a timely manner as current methods employed by AML/CTF agencies and bodies are inadequate for capturing and reporting the full plethora and scope of new money laundering and terrorism financing activities and their associated behaviours as and when they are identified.

What is required is a collaborative, synergistic reporting system that can be updated in real-time; thereby informing AML/CTF practitioners and governments immediately or soon after a new technique or method has been discovered.

Many of the shortcomings of the current reporting system could be addressed by the establishment of a collaborative, synergistic information sharing and knowledge management initiative allowing osmotic flows of information between AML/CTF practitioners and governments (including law enforcement agencies, AML/CTF regulators and financial intelligence units). This initiative should include the introduction of a central repository which holds a set of money laundering and terrorism financing behaviour models that can be extended by AML/CTF practitioners every time a new scenario, typology or Type arises. The models would assist practitioners to identify whether the case that they are dealing with fits already predefined money laundering and terrorism financing behaviours or whether a new behaviour has been discovered. These models may also be useful for the development of money laundering and terrorism financing


Business
Business turnover lower than amounts of the performed transactions.
-Manages
-Several cash deposits for very large amounts
Personal Account
Suspect
Funds appear to originate from illegal trafficking in goods and merchandise.
-Part of funds deposited invested in
-Part of funds deposited invested in
Suspect had a large capital with his bank which was inconsistent with customer profile.
Securities
Life insurance Policy

Interactions that took place were as follows:

1. ***Suspect**, who manages a **Business**, deposited several cash deposits for very large amounts into his Personal Account*
2. *Part of funds deposited into **Suspects** Personal Account were used to purchase Securities*
3. *Part of the funds deposited into the **Suspects** Personal Account were used to purchase a Life Insurance Policy*

Red flag indicators present in this case :

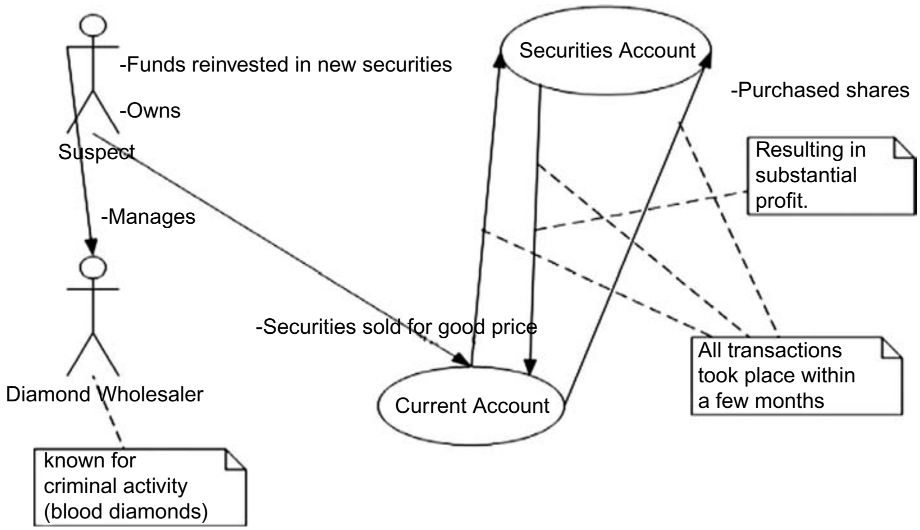
- *Transactions inconsistent with customer profile*
- *Several cash deposits of very large amounts*

Figure 8.
Investment in securities and life insurance policies to conceal commodity trafficking

detection tools and the training of new analysts or practitioners. In addition, the repository could be used to regularly register knowledge and exchange or pass on competencies, intuition, ideas and motivations to fellow AML/CTF practitioners in any part of the world.

Better knowledge would allow practitioners and governments to model, simulate and forecast financial crime, money laundering and terrorism financing more accurately and intervene more effectively to prevent it. By collecting and crossing information from different aspects and approaches, information would be transformed into systematic knowledge which, in turn, could be used to develop further information.

Although modelling can assist in understanding complex environments, the whole process of model building balances on good design that is logically and rationally grounded, reasonable in its basis and development, and sheltered from the risks coming from unsound basic assumptions, erroneous processes or distortions, all of which can produce unreliable results. To this end, a proper, standardised modelling methodology should be used by all practitioners in the development of the money laundering and terrorism financing models before they can be added to the central repository.


Securities Account
-Funds reinvested in new securities
-Owns
-Purchased shares
Suspect
Resulting in substantial profit.
-Manages
-Securities sold for good price
All transactions took place within a few months
Diamond Wholesaler
Current Account
known for criminal activity (blood diamonds)

Interactions that took place were as follows:

1. *The **Suspect**, who manages a **Diamond Wholesaler**, purchased shares for his Securities Account using funds from his Current Account*
2. *Securities from the Securities Account were sold for a good price and the funds were transferred to the **Suspect's** Current Account*
3. *The Funds from the sold securities were reinvested from the **Suspect's** Current Account into new securities.*

Red flag indicators present in this case :

- *Transactions inconsistent with customer profile*
- *Suspect known for trading in blood diamonds/criminal activity*

Figure 9. Investment in securities to conceal commodity trafficking

This paper demonstrated how complex transactional flows and interactions between the different entities involved in a money laundering and terrorism financing case can be extracted and shown in an easy-to-follow, graphical format, allowing practitioners to more easily and quickly extract the relevant information from the typology as opposed to reading a full text-based description. In addition, these models make it easier to discover trends and patterns present within and across Types and allow money laundering and terrorism financing typologies to be updated and published to the wider international AML/CTF community as and when new trends and behaviours become apparent.

Notes

1. A money laundering and terrorism financing Type is a collection of typologies that utilise the same predicate offence, method or technique.
2. There are a number of predicate offences that were not present in the random sample for this survey; however, it is believed that the information obtained is sufficient for this project.

References

Alach, Z.J. (2010), "Policing and effects-based operations: modelling methamphetamine", *Policing: An International Journal of Police Strategies & Management*, Vol. 33 No. 3, pp. 490-505.

Belgian Financial Intelligence Processing Unit (2005), *C.T.I.F.-C.F.I.: 12th Annual Report*, available at: www.ctif-cfi.be/website/images/EN/annual_report/2005_ctif_cfi_en.pdf (accessed 22 August 2011).

Biagioli, A. (2006), "Methodological innovation and effective action: looking into synergies to countering economic crime", *Journal of Financial Crime*, Vol. 13 No. 3.

Biagioli, A. (2008), "Financial crime as a threat to the wealth of nations: a cost-effectiveness approach", *Journal of Money Laundering Control*, Vol. 11 No. 1, p. 88.

Biagioli, A. and Nardo, M. (2007), "A crossroad in combating and preventing financial crime: looking for synergetic instruments for attack and prevention", *Journal of Financial Crime*, Vol. 14 No. 2.

Blackwell, L, von Konsky, B. and Robey, M. (2001), "Petri net script: a visual language for describing action, behaviour and plot", *ACSC '01 Proceedings of the 24th Australasian conference on Computer Science, 29 January-4 February*, pp. 29-37.

Chang, Y.-C., Huang, Y.-C. and Chu, C.-P. (2009), "B2 model: a browsing behaviour model based on high-level Petri-nets to generate behavioural patterns for e-learning", *Expert Systems with Applications*, Vol. 36, pp. 12423-40.

Choo, K.-K.R. and Smith, R.G. (2008), "Criminal exploitation of online systems by organised crime groups", *Springer Science, Asian Criminology*, Vol. 3, pp. 37-59.

FATF-GAFI.org (2004), *9 Special Recommendations* (*SR*) *on Terrorist Financing* (*TF*), *22 October*, available at: www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html (accessed 22 August 2011).

FATF-GAFI.org (2011), *How is Money Laundered?*, available at: www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html (accessed 23 August).

Fleming, M.H. (2009), "FSA's scale & impact of financial crime project (phase one): critical analysis", Occasional Paper Series 36, August 2009, Financial Services Authority, available at: www.fsa.gov.uk/pubs/other/critical_analysis.pdf (accessed 22 August 2011).

FSC (2009), *Money Laundering and the Financing of Terrorism*, Financial Supervision Commission, available at: www.fsc.gov.im/aml/ (accessed 22 August 2011).

Gao, S., Xu, D., Wang, H. and Green, P. (2009), "Knowledge-based anti-money laundering: a software agent bank application", *Journal of Knowledge Management*, Vol. 13 No. 2.

Global Justice Information Sharing Initiative (2006), *Fusion Centre Guidelines – Developing and Sharing Information in a New Era*, United States Department of Justice, Washington, DC.

Graycar, A. and Grabosky, P. (1996), *Money Laundering in the 21st Century: Risks and Countermeasures*, Australian Institute of Criminology, Griffith, available at: www.aic.gov.au/documents/D/D/E/%7BDDE3E02F-CF47-473D-8603-9DDC708CE4F4%7DRPP02.pdf (accessed 22 August 2011).

Hardouin, P. (2009), "Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing", *Journal of Financial Crime*, Vol. 16 No. 3.

Köhler, M., Moldt, D. and Rölke, H. (2001), *Modelling a Sociological Case Study*, available at: www2.informatik.hu-berlin.de/~lindeman/masho01_contributions/koemolroe.acrobat3.pdf (accessed 22 August 2011).

Liu, X. and Zhang, P. (2007), “An agent based anti-money laundering system architecture for financial supervision”, *IEEE Wireless Communications, Networks and Mobile Computing, WiCom 2007, International Conference on 21-25 September*, pp. 5472-5.

Mueller, R.S. (2006), “The art of information”, *Vital Speeches of the Day*, Vol. 72 Nos 14/15, pp. 434-6.

Nardo, M. (2004), “Mapping the trails of financial crime”, *Journal of Financial Crime*, Vol. 12 No. 2, pp. 139-43.

Nardo, M. (2006), “Building synergies between theory and practice: countering financial crime on a systemic approach”, *Journal of Financial Crime*, Vol. 13 No. 3.

O’Connell, P.E. (2008), “The chess master’s game: a model for incorporating local police agencies in the fight against global terrorism”, *Policing: An International Journal of Police Strategies & Management*, Vol. 31 No. 3.

Piccard, W. (2008), “Modelling multithreaded social protocols with colour Petri-nets”, *IFIP International Federation for Information Processing*, Springer, Boston, MA.

University of Aarhus (2011), *Coloured Petri Nets at the University of Aarhus*, available at: http://daimi.au.dk/CPnets/proxy.php?url=/CPnets/index (accessed 7 May).

Walker, J. (1998), *Global Money Laundering Flows – Some Findings*, available at: www.johnwalkercrimetrendsanalysis.com.au/ML%20method.htm (accessed 22 August 2011).

Wise, B.P., McDonald, M., Reuss, L.M. and Aronson, J. (2001), *Task Order* (*TO*) *69 – ATM Human Behaviour Modelling Approach Study*, available at: www.asc.nasa.gov/aatt/rto/RTOFinal69.pdf (accessed 11 July 2011).

WorldBank.org (2003), *Money Laundering and Terrorist Financing: Definitions and Explanations*, Chapter 1, 30 March, available at: www1.worldbank.org/finance/assets/images/01-chap01-f.qxd.pdf (accessed 22 August 2011).

About the authors

Angela Samantha Maitland Irwin is currently a PhD candidate of Professor Jill Slay at the University of South Australia. Her PhD is on the topic of “Money laundering and terrorism financing in virtual environments”. Angela Samantha Maitland Irwin is the corresponding author and can be contacted at: irwas001@mymail.unisa.edu.au

Dr Kim-Kwang Raymond Choo is a Senior Lecturer at the University of South Australia, and has (co-)authored a number of publications in information security, cyber crime and anti-money laundering, including a book published in Springer’s Advances in Information Security book series, three Australian Government Australian Institute of Criminology (AIC) refereed monographs, and several book chapters.

Dr Lin Liu received the BEng and MEng degrees in Electronic Engineering from Xidian University, China in 1991 and 1994, respectively, and a PhD degree in Computer Systems Engineering from the University of South Australia (UniSA) in 2006. Currently she is a Lecturer at the School of Computer and Information Science, UniSA and her research interests include Petri nets and their applications to protocol verification and network security analysis, as well as data mining and its applications to biological data analysis. She has published more than 20 refereed journal and conference papers in the aforementioned research fields.