THESIS / THÈSE

MASTER IN ECONOMICS

Analysis of inefficiencies in financial institutions detection of money laundering

LANOTTE , Myriam

Award date:
2012

Awarding institution:
University of Namur

FUNDP
NAMUR

Analysis of Inefficiencies in Financial Institutions Detection of Money Laundering

Myriam LANOTTE

Directeur: Prof. I. Linden & I. Jureta

Mémoire présenté
en vue de l'obtention du titre de
Master 120 en Ingénieur de gestion,
à finalité spécialisée

ANNEE ACADEMIQUE 2011-2012

Business Administration Department – University of Namur (FUNDP)
Member of the LSM group
Rempart de la Vierge 8, B-5000 Namur, Belgium, Tel. +32 [0]81 72 48 41/5319, Fax +32 [0]81 72 48 40

Master Thesis

Analysis of Inefficiencies in Financial Institutions detection of Money Laundering

Lanotte Myriam

Master in Business Engineering, 2nd year

June 7, 2012

Contents

List of Figures

Foreword

This Master thesis has been written during the academic year 2011-2012 under the supervision of Ivan Jureta and Isabelle Linden.

The aim of this thesis is to highlight some reasons and sources of the current lack of efficiency in the money laundering detection performed by financial institutions and to propose some recommendations to improve this detection. This investigation is based as well on the available literature in this field at the technical, financial and governmental level, as on interviews of experts in this domain.

I want to thank my supervisors Ivan Jureta and Isabelle Linden for their help, availability and their good advices. I also thank Mrs. Anne Goldfischer, Mr. Markus E. Schulz and Mr. Christian Tournie for providing through interviews invaluable information for this thesis. I would also like to thank Mr. Patrick Foissac and Mr. Oscar Bernal for their help and I am grateful to my family for their support during the writing of this thesis.

Namur, June 2012

Lanotte Myriam

Abstract

Money laundering (ML) corrupts financial markets, affects the public's confidence in the financial system and tends to create an increasingly risky market decreasing growth rate. The United Nations Office on Drug and Crime evaluates the worldwide bank fraud at one trillion dollars dollars per year. Because it costs the world economy so much, ML is becoming an important field of interest for governmental entities. Recommendations and directives are taken by international entities. These directives have to be interpreted by countries and transformed into national laws. Certain financial institutions and individuals are forced to translate these national laws into measures and procedures according to the nature of the activities of these institutions. Given the large amount of data and the complexity of the financial system, decision-support systems are needed to help experts identify suspicious transactions. This need has created a strong competition on the market of AML solutions proposing many sophisticated solutions to detect suspicious cases.

Despite the already taken measures at the governmental and financial domains and the developed systems in the technical area, experts highlight that the detection of money laundering is inefficient in financial institutions. Indeed, according to interviewed experts,Mrs Anne Golfischer (compliance officer), Mr Christian Tourni(detached expert at the European Commission) and Mr Markus E. Schulz (chief compliance officer and supervisor of the ACAMS), measures taken within financial institutions to fight against money laundering are enough to respect imposed recommendations, directives and laws but are not efficient to really fight against money laundering.

Considering this, this master thesis identifies some of the reasons for the current lack of efficiency in the ML detection performed by financial institutions at the technical (AML systems), formal (international and national entities) and informal level (motivation, implication, attitude of financial institutions toward money laundering). This investigation aims to offer some recommendations to improve the performance of the ML detection and consequently decrease its cost.

Chapter 1

Introduction

1.1 Context

The fight against money laundering is not a new field of interest. According the FATF, the Financial Action Task Force, an inter-governmental body which "has developed a series of recommendations that are recognized as the international standard for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction"[37] (see section 3.1), many regulation institutions were concerned with developing policies to fight against money laundering and to combat the usage of the financial system for drug traffic. But after 11th September 2001, this field has become more important and more oriented against financial terrorism.

Constrained by regulations and policies, European governments required a concrete implication from all financial entities of their country in the suspicious activity detection and in the production of Suspicious Activity Report (SAR). In view of the large amount of data and the complexity of the financial system, decision-support systems helping experts in the identification of suspicious transactions are needed. This need has created a strong competition on the market of AML solutions as well as a real interest in this field.

Nowadays, money laundering is becoming an extensively studied topic and more and more publications are available in this field as well in the governmental and financial area as in the technical one ([13, 14, 15, 32, 21, 20, 3, 37, 31, 45, 33, 43,

7, 24, 23, 10, 30, 8, 22, 11, 4, 29, 1]). Despite the already taken measures at the governmental and financial domains and developed systems at the technical area, a lack of efficiency in the detection of money laundering performed by financial institutions is highlighted by experts in this field met and who were interviewed during the writing of this thesis [27, 28]. Indeed, according to these experts, measures taken within financial institutions to fight against money laundering are enough to respect imposed recommendations, directives and laws but are not efficient to really fight against money laundering. This lack of efficiency is related by the United Nations Office on Drug and Crime which evaluates the worldwide bank fraud at 1 trillion dollars in one year. Considering this dramatic evidence, it appears more and more urgent as well for institutions as for nations to implement procedures and mechanisms to prevent and detect this kind of financial fraud which is more and more present and sophisticated [20].

Money laundering corrupts financial markets, affects the public's confidence in the financial system and tends to create a more and more risky market with a rate of growth which decreases [4]. Because money laundering costs the world economy so much, this master thesis aims to highlight some reasons and sources of the current lack of efficiency in the ML detection performed by financial institutions, in the purpose to offer some recommendations to improve the performance of this detection and consequently to decrease the cost for the world economy.

Different hypotheses at the technical, formal and informal level can explain this deficiency.

At the technical level, the lack could come from the technical measures taken by financial institutions to detect suspicious cases. These used AML solutions are studied in chapter 2 which aims to identify limits of these systems. Through the analysis presented in this chapter some additional qualities required for a more suitable and efficient solution are highlighted: (1) adding a learning capability to AML system, (2) adding mechanisms which can bring a more accurate detection, and (3) the need to have a system which can use different database format. This chapter also

describes some techniques and mechanisms to respond to these additional required qualities.

Secondly, at the formal level, this lack can come from the problems of strictness of interpretation of trans-national AML recommendations and directives in national laws and of the translation of these national laws into AML procedures and measures by financial institutions at the local level. These hypotheses are analyzed in chapter 3.

Lastly, this lack of efficiency could also directly come from the lack of motivation to and implication in the AML track of financial institutions. The chapter 4 presents these informal problems and highlights for example the importance that financial institutions have a positive attitude towards AML and cultivates a moral responsibility in this track, that the AML responsible people well know the banking and ML process, and that the AML staff takes time and invest to well understand the used AML software to improve its performance.

In view of these hypotheses concerning the lack of efficiency of the ML detection within financial institutions as well at the technical, formal and informal level, chapter 5 proposes some recommendations to improve the detection performance.

The contribution of this thesis lies in the span of analysis across the informal, formal, and technical domains. Indeed, current researches about money laundering are mostly based on one of these three system: the technical articles presenting systems don't care about the legislation around money laundering, nor about the technical capabilities of AML staff in financial institutions, the legislation don't care about methods used by financial institutions to respect it, etc. . Thanks to an anlysis taking into account several interrelated domains a more complete and realistic view of the reasons for the lack of efficiency of the ML detection is provided.

Various topics can be studied in relation to fraud detection but I have focused this work on the detection of suspicious activities related to money laundering by financial institutions. No other techniques to fight against suspicious activities (e.g. the study of social networks, etc.) are explored in the present survey. This is not to suggest that this topic is not important. But I would like to limit the scope of this

thesis to the identification of the sources for the lack of efficiency of the detection of suspicious activities by financial institutions. I'm convinced that staying focused on this limited area could perhaps bring more limited but also more precise results. Moreover, financial institutions play a major role in the AML fight.

Regarding the methodology used to write this essay, I principally took stock of the available literature. No analysis based on really implemented AML solutions is performed. The reason for this choice is not a lack of interest, but only the secrecy about AML solutions. Through some meetings with financial entities and solution providers, I could perceive the sensitive side of this area.

In the rest of this chapter, firstly, the money laundering is defined and situated among other financial frauds with the aim to establish the scope of the analysis proposed in this thesis. Secondly, the ML process is presented in the purpose to highlight the complexity of this one and the number of actors and entities implicated in this process. Thirdly, this complexity being increased by the number of tools and techniques which can be used by money launderers within this process, the most common ones are described.

1.2 Important Concepts

Before going on with the research question, let us define the most important used concepts. The first ones include the definition of the concept of fraud and the position of money laundering among the other kinds of fraud. Next, the concept of money laundering (ML) is defined. Moreover, the ML process and the different tools and techniques used by money launderers are also exposed. Lastly, the TFI framework is presented. This framework is considered as the cornerstone for the whole analysis performed in this work.

1.2.1 Fraud

A) Definition

There is not only one definition of what a financial fraud is [25]. Let us analyze some of them.

- The Oxford English Dictionary [2] defines a financial fraud as *" a wrongful or criminal deception intended to result in financial or personal gain"*. This definition reveals two important characteristics: the criminal character of a financial fraud and the goal, a personal gain.
- A financial fraud is also identified as *"a deliberate act that is contrary to law, rule or policy with intent to obtain unauthorized financial benefit"* [19]. Through this definition, a financial fraud is one more time identified as contrary to the law and with the aim of financial benefits. Moreover, the "*deliberate*" character of the fraud is highlighted.
- Finally, [9] characterizes the financial fraud as *"the abuse of a profit organization's system without necessarily direct legal consequences"*. This definition expresses the abuse of a financial system.

Summarizing these definitions, in this work, we consider as a financial fraud every deliberate criminal act which abuses a profit organization's system with the aim of personal and financial gains.

B) The Different Kinds of Fraud

Figure 1.1 illustrates four categories of financial fraud: bank fraud, insurance fraud, security and commodities fraud and other types related financial fraud [25] and for each category distinguishes different fraudulent activities including Credit Card Fraud, Money Laundering, Automobile Insurance fraud, Crop Insurance fraud, Healthcare insurance Fraud, mass marketing fraud or Corporate Fraud.

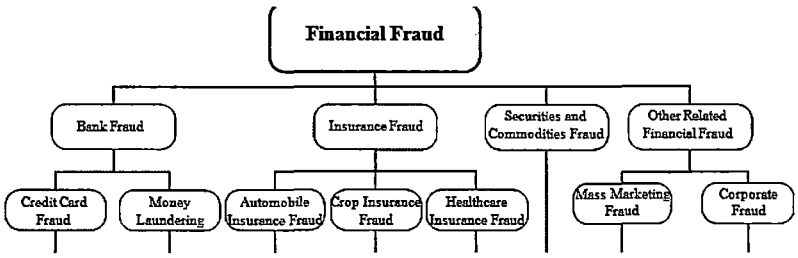

Figure 1.1: The different kinds of fraud [25]

Notice that, money laundering is included in the Bank Fraud category. This category is defined by Connell University Law School (CULS) as *"whoever knowingly executes, or attempts to execute, a scheme or artifice (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises."*

1.2.2 Money Laundering

After having situated money laundering among other kinds of fraud, this subsection proposes a better understanding of the concept of money laundering through first a definition of what is called "money laundering" based on several definitions proposed by different authors. Then the process of money laundering is presented through its three stages: the placement, the layering and the integration. Finally, the most common tools and techniques used by money launderers are exposed.

A) Definition

The FBI describes money laundering as *"the process by which criminals conceal or disguise the proceeds of their crimes or convert those proceeds into goods and services. It allows criminals to inject their illegal money into the stream of commerce, thus corrupting financial institutions and the money supply and giving criminals unwarranted economic power"* [25].

Money laundering is also characterized as *"a process to make illegitimate income appear legitimate; this is also the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activity"* [21].

The HM Treasury defines Money laundering as *" the term usually used to describe the ways in which criminals process illegal or "dirty" money derived from the proceeds of any illegal activity (e.g the proceeds of drug-dealing, human trafficking, fraud, embezzlement, insider trading, bribery, theft or tax evasion) through a succession of transfers and deals until the source of illegally acquired funds is obscured and the money takes on the appearance of legitimate or "clean" funds or assets"* (HM Treasury, 2004 cited by [15]).

Through the previous definitions we can highlight the following important elements characterizing money laundering:

- Hiding the origin and the ownership of illegitimate activities' benefits in transforming dirty money into clean funds ;

By the following means:

- Disguising benefits of a crime in converting those benefits into goods and services ;
- Inserting illegal money into the economic system by means of a succession of transfers and deals;

B) Process

The ML process is a complex process involving many actors in many countries using many accounts in many financial institutions [26]. This subsection describes the different stages composing this process highlighting its complexity. This description allows to understand the international aspect of the ML detection and the importance to have an implication in the ML track by all financial institutions of all countries together to efficiently detect money launderers.

The money laundering process can be viewed as a cycle of three money laundering stages: the placement, the layering and the integration [15, 8]. The placement (the first stage) performs the transfer of illegal benefits into the financial system avoiding detection by transforming physical currency into other assets (ex: via business activities...). The goal of this step is to remove funds as far as possible from its

origins [4]. The layering (the second stage) tries to create distance from the source of the illegal activities in generating many layers of transactions. The layering create a web of financial transactions for the purpose of looking like legitimate financial activities [4]. Finally, the integration (the third stage) ensures the reinsertion of laundered money into the economy. This stage is performed by "aggregating illicit funds from various legitimate commercial activities and financial systems".

This process is represented in figure 1.2.

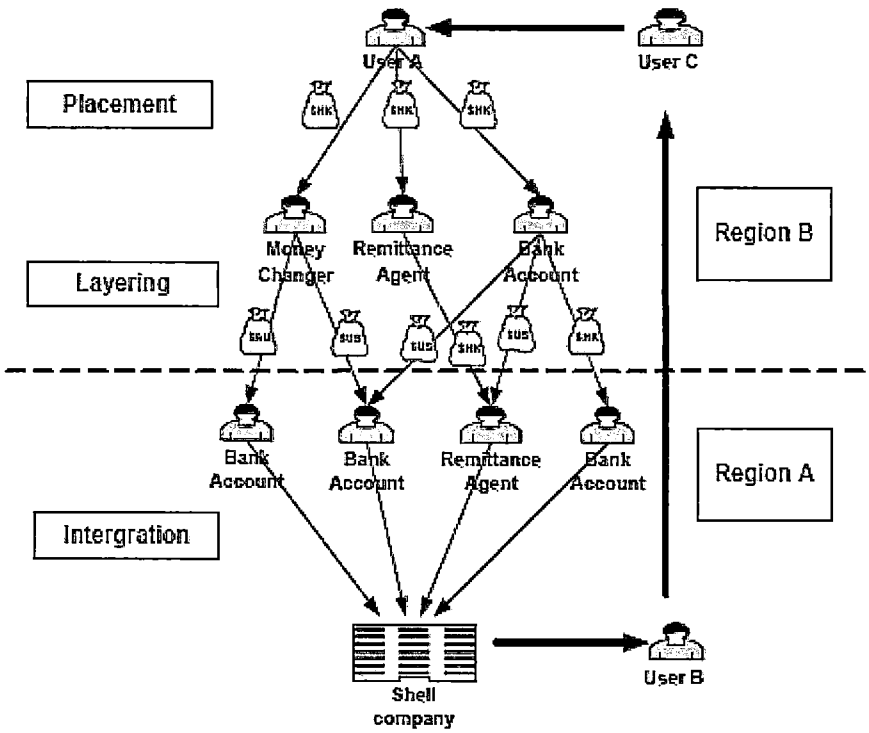

Figure 1.2: Money Laundering procedure [8]

As illustrated, the ML process involves many agents and integrates many entities (companies, banks, etc.). At each stage, the laundered money placed in a bank account involves a financial institution. Consequently, at the end of this process, many institutions have been involved in the money laundering. The detection is more difficult at the beginning of this process (placement and layering stages) because the amount of money to launder is divided in many small sums difficult to detect. In contrary, at the end of this process (at the integrating stage), all these small sums are aggregated to be integrated in the financial system. In this level, the amount

of money in higher and the placement on a bank account is tricky. Indeed, it's confronted to a large amount of money that the origins are analyzed, that the profile of account's owner are studied, etc. Consequently, it's at this level that the detection is the more conclusive [26].

C) ML Tools and Techniques

The complexity of the ML process is increased by the more and more advanced techniques used by criminals. Moreover, even if money laundering was some years ago limited to personal gain from the drug traffic, now this term also points out financial terrorism [4]. Common techniques and tools of money laundering can be summarized through Structuring, Front companies, Misinvoicing, Shell companies, Wire transfers, Mirror-image trading, and Parallel systems [4].

The first technique,*Structuring*, refers to the division of large deposit (over 10,000 dollars) to avoid reporting required for all transactions over 10,000 dollars. The use of *front companies* can also be useful to money launderers because such companies do not necessary need financial institutions and these companies can also perform legal activities making it difficult to detect ML. The *misinvoicing* of international trade transfers is another common technique of money laundering. The fourth technique is the use of *Shell corporations.* The term "Shell corporation" is defined by the Financial Action Task Force as a corporation or institution "that does not conduct any commercial or manufacturing business or any form of commercial operation in the country where their registered office is located". Next, the use of *electronic funds transfers* or wire transfers is another mean to layer illicit funds. *The mirror-image trading schemes* "involves buying contracts for one account while selling an equal number of contracts from another one. Both accounts are controlled by the same person, thus any profit or loss is effectively netted". Finally, it is also possible that laundered money never transits through the mainstream financial system but through "an underground banking system such as the Hawala and Hundi system in India or parallel banking systems in China"[4].

It's important to notice that these tools and techniques constantly evolve and

adapt themselves to the detection [26].

The current analysis concerns techniques and tools involving the mainstream banking system: the structuring, the misinvoicing, electronic transfers, and the mirror-image trading schemes and the use of shell corporations.

1.3 The TFI Framework in ML

The previous sections of the introduction have presented the definition of the concept of money laundering, its process, the common used tools and techniques and its position among other kinds of fraud.

In this section, an important framework considered as the cornerstone for all the analysis of the lack of efficiency in ML detection is proposed. This framework is called the TFI framework [5]. This one is illustrated by figure 1.3.

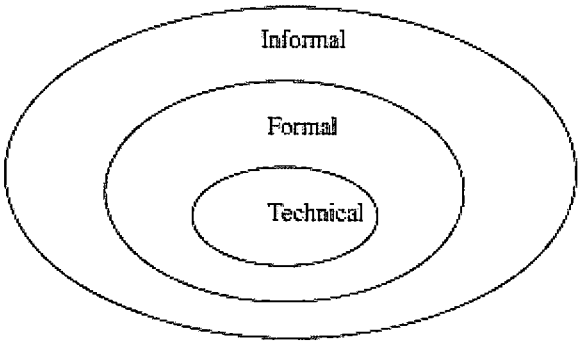

Figure 1.3: TFI framework [5]

"The TFI model conceptualizes an information system as being itself comprised of three different but interrelated systems" [5]. Its name refers to the three systems composing this model: the technical system, the formal system and the informal system. This model illustrates the fact that a technical system (hardwares, softwares, protocols, technology design, interfaces, etc) is embedded in and influenced by a formal system (attributes of the system which are documented and formalized in rules, procedures, etc) which is itself embedded in and influenced by an informal system (culture, beliefs, values of the members of the system) [5].

This framework can be applied to money laundering and allows us to understand the relationships between the technical AML solutions, the regulations around it and the AML staff and departments composing the informal environment around technical solutions. In the context of AML systems, the technical level consists of AML softwares. The formal level involves norms as well at the trans-national level as at the national one. Finally, the informal level consists on the attitudes and beliefs towards money laundering, the motivation, the moral responsibility and the implication of the AML staff [5].

Table 1.4 applied the TFI framework to money laundering.

TFI in ML	
Level	Factors
Technical	Adoption of ML profiling is surrounded by both technical and economic ambiguity.
Formal	Abundance of norms at the transnational, national and local level, Abstract norms are interpreted according to particular priorities and interests.
Informal	Generalised disbelief in the goals of the activity, as well as the effectiveness of the tools being used. Attitude vary with size of banks and the nature of activity, but not with prior existence of AML tools. Pacement of the AML decision maker at board level seems to offer legitimacy and facilitate the avaibility of resources. The treat of fines, as opposed to actual fines, also seem to influence action.

Figure 1.4: TFI in ML [5]

Through this framework it's easier to understand that not only AML technical solutions are responsible for the lack of efficiency of ML detection. Indeed, the technical aspect of ML detection is embedded in two other systems; the formal system relating regulation actors and the informal system which is more oriented to AML staff, their motivation and implication in the ML detection. As explained, "group acting in different informal environments react differently to the same formal or technical element" and then a same technical solution can be more or less efficient according to its formal and informal environment.

Based on these interrelated systems and on the evidence that not only technical systems are responsible for the lack of efficiency of the ML detection exercise, the analysis presented in this thesis is divided into three levels: the technical level, the formal level and the informal one. Moreover, this thesis highlights the relation and the dependence between these systems. This interdependancy is often forgiven in articles about money laundering which only deal with one system (the technical

in proposing softwares, the formal in proposing directives and legislations , or the informal in explaining difficulties within financial institutions).

1.4 Structure of the Work

This introduction has firstly presented the scope of this work situating money laundering among the other kinds of frauds. Secondly, the presentations of the ML process and of the common used ML techniques and tools have highlighted the complexity of this field involving many agents, many entities in many countries. The last section of this introduction has proposed the TFI framework applied to money laundering highlighting the importance of an analysis based on the three independent and interrelated systems (the technical, formal and informal systems).

In the purpose to identify the sources for the lack of efficiency of the ML detection performed by financial institutions, these three areas (technical, formal and informal) are investigated through chapters 2, 3, 4.

Chapter 2 presents the technical AML system. It firstly identifies the limits of currently implemented systems which could decrease the detection performance and which are highlighted by interviewed experts. Next, these limits are translated into additional required qualities for a more efficient and suitable AML software. Finally, through the investigation of new AML solutions proposed by the literature, some techniques are proposed to respond to the highlighted required qualities with the aim to improve the ML detection at the technical level.

Chapter 3 highlights limits for an efficient ML detection at the formal level. This chapter identifies two sources for the lack of efficiency at the formal level: (1) the lack of strictness in the interpretation of international recommendations and directives into national laws, and (2) the lack of strictness in the translation of these national laws into measures and procedures by financial institutions at the local level.

Chapter 4 explores the informal AML system with the goal to find some possible sources for the lack of efficiency of the ML detection at this level. Through two surveys and two interviews, some informal aspects are investigated in the purpose to highlight their influences on the ML detection performed by organizations: the

impact of the culture of organizations, their attitude towards money laundering, the implication and the motivation for the ML track from the senior manager, and the AML staff capability, awareness and knowledge of anti-money laundering tools (technical AML system), ML process, banking process, etc.

After the identification of some sources and reasons for the lack of efficiency of the ML detection at the technical, formal and informal level, chapter 5 proposes some recommendations for each level to improve this detection.

Chapter 2

The Technical AML System

Financial institutions are required to translate national AML laws into procedures and measures to detect ML cases (see chapter 3) [14, 15]. One measure is the use of technical systems. Indeed, considering the complexity of the ML process (see subsection Process in section1.2.2), the amount of tools and techniques used by money launderers which constantly evolve (see subsection ML tools and Techniques in section1.2.2), and the large amount of transactions and accounts to deal, the use of a technical AML software is required to perform an efficient detection.

As explained through the TFI model (section 1.3), the technical system is the most embedded one in the ML information system. This technical aspect is presented in this chapter. In the purpose to identify the sources for the lack of efficiency of the ML detection which can come from the technical system, some experts are interviewed and the already implemented techniques are analyzed in the purpose to highlight the possible current limits of those systems which could decrease the detection performance. These limits are translated in additional required qualities for a more efficient and suitable AML solution. Finally, some techniques are proposed to respond to these required qualities.

2.1 The Market of AML Solutions

Since September 11, 2001, more and more AML solutions are proposed on the market of AML solutions creating a strong concurrency. In addition to SAS with their "SAS Anti Money Laundering" other providers are present with other solutions as ACI with their " ACI Automated Case Management System for Anti-Money Laundering [33], Norkom with their "Norkom's Anti-Money Laundering (AML) solution" [39], Fiserv [36],I-sight [38], Mantas Inc.,

Figure 2.1 presents a ranking of the most important AML solutions currently implemented on the market [6]. Each provider propose a different solution but all these systems include some similar components as the following ones: the customer knowledge, transaction control, conformity report, investigation tools [43].

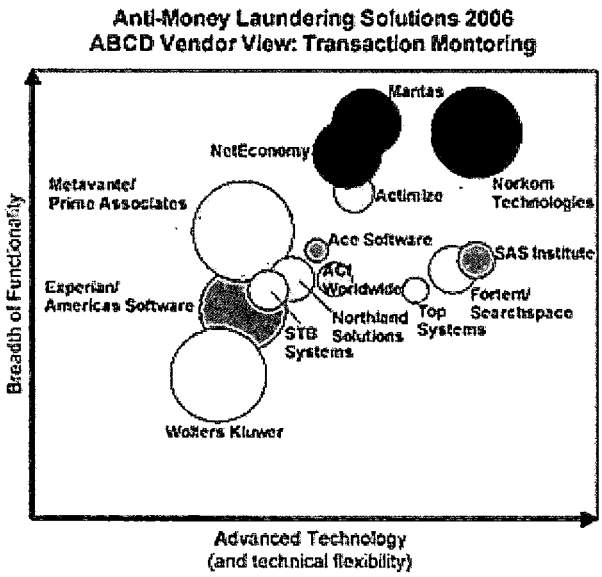

Figure 2.1: AML Solutions 2006 [6]

2.2 Used Techniques in Currently Implemented AML Solutions

According to the experts in fraud detection interviewed for this analysis [27, 26], these solutions are confronted to some limits. Indeed, these experts reveal that de-

cision support systems currently implemented to fight against money laundering are enough to respect imposed recommendations and directives but are not efficient to really stop money laundering. Indeed, these systems forgiven that the human expertise takes the major place in the ML detection. They only consider the technical mechanisms [27] without reintegrating the human expertise performed in previous detection to improve future detection. Another highlighted problem [26] is the fact that these provided solutions require a specific database format. Therefore financial institutions have to adapt their database to the implemented AML system. Moreover, they produce too much errors in the detection and consequently a waste of time for human experts [27]. Another interviewed expert [28] moderates these assertions and considers that currently implemented solutions could be improved but are already efficient if they are correctly and efficiently used. For this expert, it's not a lack of efficiency of proposed tools but in the use of these tools which require being configured according the nature of activities of the institutions which use it. This configuration requires a technical knowledge in addition to knowledge in the ML and banking process. According to this expert, it's really rare to find all this knowledge aggregated in a same AML team of an organization.

In sum, these experts highlights different problems of currently implemented AML solutions: (1) a lack of learning based on previous detection performed by human experts, (2) a specific database format required, (3) a configuration which is difficult, and (4) too much errors in the detection (too much false positive and false negative suspicious cases).

This section aims to understand from where come the limits highlighted by the interviewed experts. In this purpose, some articles from the literature in this field [13, 14, 15, 32, 21, 20, 25, 7, 24, 23, 30, 8, 22, 5, 4, 19, 9, 18, 44] describing some techniques used in currently implemented AML solutions and their limits are used.

2.2.1 The most Common Used Techniques: Description and Limits

This literature reveals that the majority of proposed solutions are based on data-mining tools to detect and predict ML cases.

"Data mining techniques are suited for identifying trends and patterns in large datasets" [16] cited in [21]. The detection of ML patterns through financial transactions require techniques which can detect suspicious cases among a large amount of data taking into account a large amount of dimensions (customer x product x geography x time). These requirements can be met by data-mining techniques. Indeed, these methods can be as well predictive as descriptive. It means that some future trends and some current characteristics, profiles hidden by the large amount of data can be highlighted.

Many predictive and descriptive methods as clustering, outlier detection, support vector machine (SVM), histogram analysis based on a discretisation process, correlation analysis, visualization, decision trees, link analysis, etc. are today implemented in AML solutions to detect or predict unusual customer behaviors.

As already mentioned above, the interviewed experts have highlighted the following limits to theses currently implemented solutions: (1) a lack of learning based on previous detection performed by human experts, (2) a specific database format which is required, (3) a configuration which is difficult, and (4) too much errors in the detection (too much false positive and false negative suspicious cases). Let us explain these limits.

A) A Lack of Learning

The investigated literature reveals that the majority of implemented solutions are predefined rule-based solutions.

These rules are build based on governmental list of risky countries, people, professions but also on rules created by financial institutions themselves to detect suspicious cases according the nature of their activity (e.g. the amount of money of a

transaction considered as suspect for a certain profession) [26].

Due to the predefined aspect of these rules, each time laws change, the system has to be redesigned and reconstruct to stay efficient in the ever changing ML context. Moreover, due to their static and predefined characteristics, these rules can be easily learned and evaded by money launders [24].

Another problem presented by these rules-based solutions is their inability to learn or generalize. Indeed, Solutions using this technique cannot learn and generalize new patterns or integrate previous performed detections as rules for future detections. They can only match patterns that they already know [14, 15].

The articles [14] and [15] also notice that solutions based on predefined rules present an inability to detect ML schemes of smaller amount. This can be linked to ineffective thresholds proposed by the rules [28].

These solutions also suffer of high false positive problems. Indeed, too many transactions are marked as suspicious but are not [14, 15].

B) A Specific Database Format

Another most important problem with currently sold solutions is the fact that to be implemented into financial institutions, they need to have a specific database format available. Therefore, financial institutions have to transform their currently used database to suit with the technical proposed AML solution [26].

C) Configuration Difficulties

The used solutions have the capacity to deal with large datasets with many attributes and dimensions but need a parameter selection by the user to be performing [28] (e.g for the clustering, the user has to select the number of iterations, the number of clusters, the seed parameter, etc. [12]). This parameter selection is complicated for people who have no knowledge in data-mining. And this parameter selection is directly linked to the expected result. Therefore, it's needed to know what you are looking for, what you really expect from the used tool, what a data-mining specialist with no knowledge in the ML and banking systems can't do.

D) Too many Detection Errors

The detection performed by investigation tools conducts to too many false positive suspicious cases [26]. Therefore, human experts have to control all these cases even if they are not suspicious in reality.

The hypotheses for this too high rate of errors can be: (1) a clustering result which is not accurate enough, (2) a lack of learning capability which can reintegrate the results of previous detections, and (3) a lack of mechanisms bringing additional knowledge which can be helpful for future detections.

First, in used data-mining tools, suspicious activities detection is essentially seen as an outlier detection problem in certain solutions [24, 45]. Nevertheless, a simple detection of suspicious money laundering transactional behavior patterns cannot be only made by means of a simple clustering or local outlier detection. Indeed, when a clustering is performed, two categories can be identified: large and small category. These categories respectively represent normal transactional behavioral patterns and abnormal ones. In the point of view of local outlier detection, all subjects of the small category are outliers compared to those in the large category. But this categorization cannot be applied to all industries i.e. for some industries normal and abnormal behavioral patterns depend on the period (seasonal industries, etc).

Secondly, this amount of errors can also come from the fact that decisions of experts about cases that the system had detected as suspect are not reintegrated into the system to improve future detections. If these decisions were reintegrated in the system, the false positive suspicious cases already detected in previous investigations would be considered by the system has not suspicious. By this learning mechanism the detection could be more accurate and the number of false positive would be decreased.

Lastly, mechanisms allowing link analysis, sequences of transactions identification, correlation and trends analysis, visualization, the calculation of the probability

of suspicion for a kind of transaction or account, etc. could be used in addition to traditional classification tools to create additional knowledge which can be stored and reused by the system for future investigation and which can consequently provide a more accurate detection.

Currently, some of these mechanisms are already used but are confronted to some limits.

For example, link analysis tools are already used in investigation to discover information about criminals and criminal's networks (e.g.: Offenders of the same supply chain)[8]. "The main function of link analysis is to retrieve information from raw data which is related to entities such as bank accounts, telephone records and criminal reports. The data is then processed and presented in a structured format. Link analysis further analyzes the information and identifies the relationship between the entities.[...] Link analysis can be time-consuming and requires substantial amount of manual work. Commercial software's labeled as link analysis tools only provide functions for visualizing manually constructed criminal networks. In these systems, associations between entities are often required to be input by the user manually "[8]. These systems "provide generic functions for all types of crimes and heavily rely on user's expertise on the domain knowledge of the domain of the crime for successful detection. As a result, they are less effective in detecting patterns in certain crimes"[8]. Moreover, association analysis can be extremely time-consuming for large dataset. This issue conducts to a lack of effectiveness in the detection of patterns for certain crimes [8].

Moreover, currently, data are only treated in an individual level; no analysis is performed based on a sequence of transaction which could reduce the number of false negative. Indeed, some transactions which is not considered as suspect in isolation could be if they are in sequence of transactions with similar characteristics.

2.2.2 In Sum

In the field of AML and financial terrorism, the final decision is to decide if a transaction is suspect or not and if this one needs of specific actions or not. This domain can be characterized by a large amount of data, many dimensions to take into ac-

count and a really quick data flow. Moreover, it's a domain wherein each error has important consequences for the economy. Hence, it is necessary to develop systems which efficiently detect and alert suspicious behaviors through transactions and operations, and which allow to treat these suspicious behaviors. It's an action decision specific for each behavior or transaction that has to be taken by several specific experts. This decision is based on report from the system, and also on knowledge and experience of experts.

According to interviewed experts, many limits to currently implemented AML system can be highlighted: (1) a lack of learning based on previous detection performed by human experts, (2) a specific database format required, (3) a configuration which is difficult, and (4) too much errors in the detection (too much false positive and false negative suspicious cases).

These limits reflect some additional important qualities required for a more efficient AML solution which would be more suitable for the ill-structured, changeable and complex ML and financial systems.

These technical requirements are the following ones: (1) adding a learning capability to AML system, (2) adding mechanisms which can bring a more accurate detection, and (3) the need to have a system which can use different database format.

Concerning the difficulties to configure systems, a solution could be bring in each financial institution at informal level (see chapter 4).

A) A Learning Capability to AML System

Most of currently implemented solutions use only predefined rules and have no learning or generalization capabilities. These solutions are confronted to some problems.

First, these solutions require too much business redesign and reconstruction each time rules change.

Moreover, these techniques due to their static aspect are too easy to learn for money launderers.

Finally, the human expertise performed in previous investigation are not reinte-

grated in and reused by the system for future investigation which is a waste of time for human experts who have to control all detection from the system.

These limits are particularly problematic in the ever changing ML context where money launderer's techniques constantly evolve and which involves a large amount of transactions to investigate.

A more intelligent, real-time, dynamic and self-adaptable technique with learning and generalization abilities is then required. By its learnability this system could learn and generalize new patterns from previous detections and not staying with patterns they already know and which are integrated through static and predefined rules.

B) A more Accurate Detection

In the purpose to perform the detection with a minimum of errors (a minimum of false positive and negative detected cases), some techniques can be used to bring additional knowledge which could be stored and reused for future detection and which can bring more accurate detection results. The following mechanisms can be used in this way: link analysis tools, correlations and trends identification tools, mechanisms to calculate the probability of suspicion of a kind of account or transaction, sequence analysis tools, etc.

C) Different Database Format

It should also be useful for financial institution to have a system which doesn't impose a strict database format. Indeed, it's really constrained for financial institution to have to change its database format to fit with the implemented AML solution [26].

2.3 New Proposed Solutions

Considering criticisms formulated by interviewed AML experts about the inefficiency of AML solutions currently available on the market, section 2.2 has highlighted some additional qualities (not available in currently developed solutions) required for a

more efficient AML solution. These requirements are the following ones: 1) adding a learning capability to AML system, (2) adding mechanisms which can bring a more accurate detection, and (3) the need to have a system which can use different database format.

In this section, we present some techniques which can provide these required qualities. These techniques come from the investigation of new developed AML approaches proposed by the literature [13, 14, 15, 32, 21, 20, 25, 7, 24, 23, 30, 8, 22, 5, 4, 19, 9, 18, 44].

2.3.1 A Learning Capability

This subsection presents some techniques which can bring a learning capability to AML solutions: the use of knowledge repositories and neural network, and the use of intelligent agents.

A) The Use of Knowledge Repositories and Neural Network

The articles [21, 20] propose a knowledge based framework using a combination of data-mining (DM) and natural computing techniques. This framework integrates learning capabilities through the use of knowledge repositories which record the results of previous detections of ML patterns, cases, behaviors, etc. Moreover a neural network is also used to provide an accurate classification based on the result on previous detection.

Figure 2.2 presents this framework which can be seen as a succession of three steps/layouts: The pre-processing, the Data-Mining and the knowledge management.

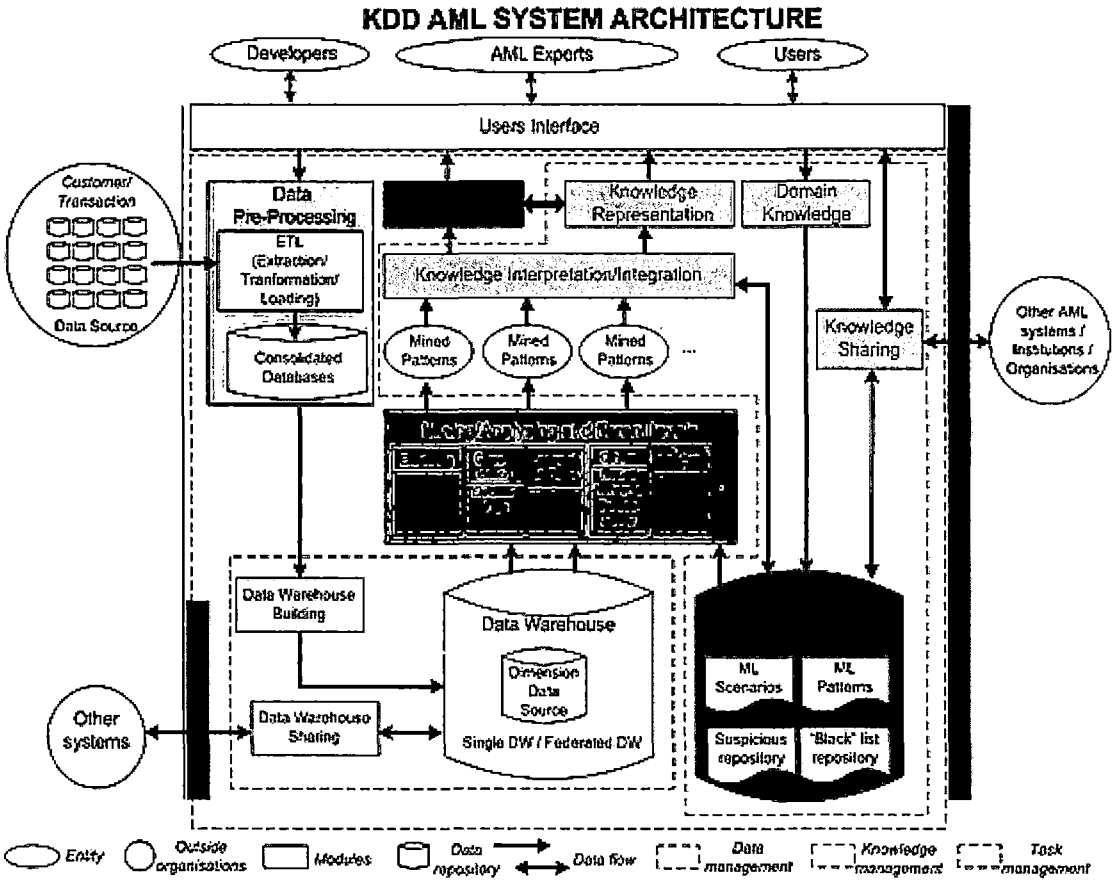

Figure 2.2: DM Architecture for detecting AML [21]

The preprocessing represents the ETL process (Export Transform and Load). This process consists on the extraction of data from data sources, the cleaning of those ones, and the integration in a data warehouse of customer information and transactions.

The data-mining layer provides data-mining techniques to analyze transaction datasets as well at a descriptive level as at a predictive one. Transactions records are extracted from the data warehouse for analysis. In this level, aggregation of transactions with individual account, are also performed and provide additional information about the financial activity of an individual. "Clustering groups similar transactions and builds suspicious profiles; classification classifies customers into pre-defined categories of risk [21]". In the purpose to provide an accurate classification, a neural network is used. The outputs of previous detections (the final decision, taken by human experts, based on potentially suspicious cases provided by the system)

are used by the neural network to create a ranking of the new potentially suspicious cases detected by the system. This ranking is based on the suspicious degree linked each detected transaction according previous detections (false positive cases or false negative cases).

The last layer, the knowledge management, represents the result of the previous investigations complemented with AML experts 'experience stored and analyzed. In this layer, rules and knowledge are generated. Different strategies are proposed to increase the performance. "For example, it integrates clustering results and learning results to build a decision tree for predicting suspicious cases [21]".

In sum, the results of previous detection (the final decision, taken by human experts, based on potentially suspicious cases provided by the system) are stored in knowledge repositories. This knowledge is used to calculate a degree of suspicious for transactions of a certain kind. This calculation is used by a neural network which establish a ranking of detected transactions. This learning mechanism provides a more accurate classification.

B) The Use of Intelligent Agents

The article [14] proposes a real-time exception management decision model which uses intelligent agents and their properties to provide an intelligent, self-adaptable, flexible, autonomous, reactive and proactive model able to learn.

This model combines three approaches: (1) the known making-decision model - the Simon's model - adapted to the ML environment which in the intelligent agent technology is applied [13], (2) The Cynefin Sense-Making framework [14] and (3) BAM logical layered architecture [14].

The Simon's model is constituted by four phases [15]: the intelligence phase, the design phase, the choice phase and the review phase. This model can be adapted to the ML environment in using intelligent agents (IAs). Due to the complexity, the structure of AML, the large amount of data, etc, IAs can be useful to analyze all transactions with the needed corporate authority to access to any data. In-

deed, thanks to their proactivity and reactivity, they are able to detect suspicious behaviors hidden among voluminous data[15].

As defined by the French Normalization Association, an intelligent agent is "an object using artificial intelligence techniques: it adapts his behavior to its environment and acts as a learning sub-system by memorizing its anterior experience. It enriches the system it uses by adding automatic functions treating, controlling, memorizing and transferring information." IAs are able to act without human intervention or intervention of another system. These agents have a control on their own intern state and on their environment [13]. Properties of an IA are the following ones: an IA is autonomic, enable to communicate and cooperate, enable to reason and react to its environment and is mobile. It also includes one or more of the following elements: a predefined knowledge base, and an inference motor (which allows having complex reasoning). Moreover, it can also include a knowledge acquisition system and a learning mechanism [17]. A multi-agents system (MAS) is group of agents which interact together in a specific environment to reach together their goals. They take other agents knowledge and capabilities to fill their own limits [15].

The second approach on which the Real-time Exception Management Decision Model is based is the Cynefin Sense-Making Framework. This framework provides a help for unspecified problems and allows to classify them. This framework is divided in several domains: - known - "known causes and effect. Cause and effect relationship are generally linear". - Knowable- "knowable causes and effects. While stable cause and effect relationships exist in this domain, they may not fully know, or they may be known only by limited group of people". - Complex- "complex relationships. There are causes and effect relationships between the agents, but the no. of agents and the no. of relationships defy categorization or analytic techniques. Emergent patterns can be perceived but not predicted". - Chaos - "there are no perceivable relationships, the system is turbulent, there is nothing to analyze; and, waiting for patterns to emerge is a waste of time." According to these different types of domain the proposed decision model has to act differently.

For a Known domain, the decision model has "to sense incoming data, categorize that data, and then respond in accordance with the predetermined practice". For

un knowable domain the decision model has to sense incoming data, analyze that data, and then respond in accordance with expert advice or interpretation of that analysis". For a complex domain, the decision model has "to create probes to make the patterns or potential patterns more visible (sense) before we take any action (respond). And for a chaotic domain, the model has "to act, quickly and decisively, to reduce the turbulence; then to sense immediately the reaction to that intervention so that we can respond accordingly".

The third approach used in the build Real-Time Exception Management Decision Model (RTEMDM) is the basic BAM logical layered architecture. Which include three layers: the Event Absorption Layer, the Event Processing and Filtering and the Event Action, Delivery and Display. BAM is defined as "providing real-time access to critical business performance indicators to improve the speed and effectiveness of business operations. Unlike traditional real-time monitoring, BAM drams its information from multiple application systems and other internal and external sources, enabling a broader and richer view of business activities"'[14].

The figure 2.3 presents the model.

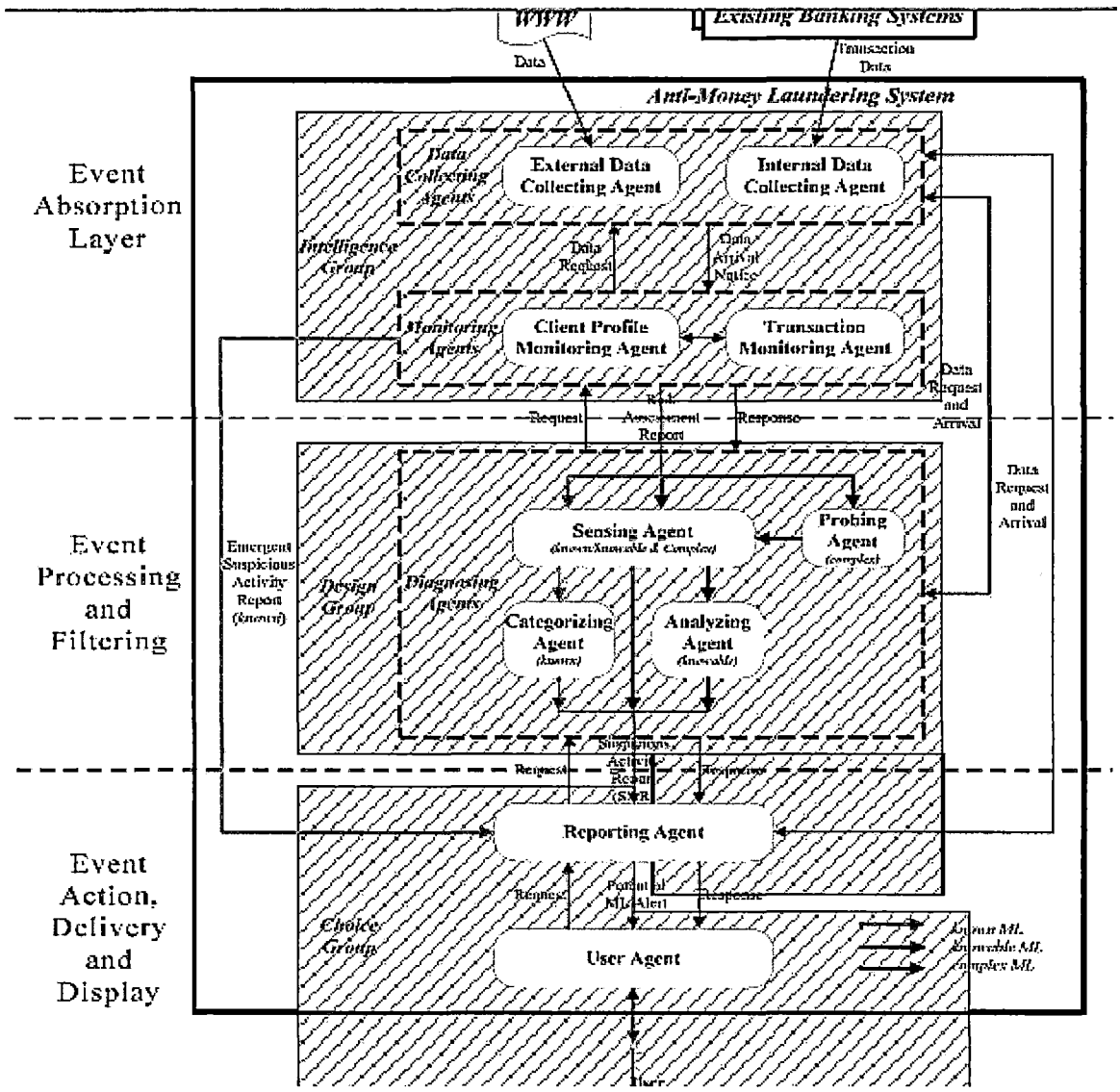

Figure 2.3: RTEMDM [14]

A seen in the figure 2.3, in the intelligence phase, two monitoring agents are presents; a client profile monitoring agent and a transaction monitoring agent. The purpose of these two monitoring agents is to provide a risk assessment report. This one will be send to agents in the following phase; the design phase.

The design phase processes according to the different types of ML indicators: in the case of known or knowable ML indicators; the categorizing agent categorizes the known activities based on existing pattern. The analyzing agent is responsible for knowable activities. This one can find suspicious patterns behind large amount of

data. In the case of complex ML indicators, the risk report produced by monitoring agents is send to the probing agent of the design phase. This agent rank customers according their degree of suspicious. The discovered pattern is send to the sensing agent to identify suspicious behaviors [14].

In sum, by their own properties, intelligent agents can bring by themselves learnability and self-adaptability. These properties are completely suitable for the ML context. Indeed, thanks to business rules and business strategies extracted from business model which constitute the specific knowledge of intelligent agent, those ones are able to reason about business actions for AML. The implementation of business rules into intelligent agent makes them able to act autonomously with flexibility and adaptability [15]. Based on situational awareness and real-time decisions, each agent manages its specific goal and is able to interact with other agents [13].

2.3.2 Mechanisms for a More Accurate Detection

The second additional quality required for a more suitable and efficient solution is the integration of mechanisms which can decrease the number of false positive and negative suspicious cases detected by the system

In the purpose, some solutions are proposed:(1) the integration of a learning mechanism, (2) of a local outlier factor algorithm, (3) of a sequence matching, (4) of visualization tools, and (5) the integration of algorithms which calculate the degree of suspicion of a person and the degree of association between two entities.

A) The Use of the Learning Capability

The learning capability which is added to system (see subsection 2.3.1) can provide an accurate classification, thanks to the additional knowledge they bring based on previous detections.

As presented, the learning capability of a system can bring additional knowledge as a ranking of detected transaction according their degree of suspicion, the previously detected ML patterns, the previously detected suspicious cases and behavior, etc.

B) The Use of a Local Outlier Factor (LOF) Algorithm

In many AML solutions, the classification is seen as an outlier detection problem [45]. In these solutions, the clustering process categorizes analyzed points into two categories: the small category (SC) and the large category (LC). The SC is composed by points with an abnormal behavior while LC includes points with a normal behavior. But points of SC are not all suspicious [45].

Therefore, [45] proposes an outlier factor (LOF) algorithm. This algorithm "measures the deviant degree of point of the small category (representing points with an abnormal behavior) from large category (representing points with a normal behavior)". More the analyzed point deviate from the LC, the higher the LOF value is. When all points have received their LOF value, the information about how the transaction is suspicious is then available. It's also possible to rank possible suspicious transactions (detected by the clustering) in function of their LOF value.

This mechanism provides an accurate classification with less false positive.

C) The Use of a Sequence Matching

The amount of false negative and positive can be decreased by a sequence matching. Indeed, according to [24], the history of each transaction of each account and transactions information from other accounts in a peer group can be used to identify suspicious sequences from large volume of transactions.

Viewing transactions as temporal sequences allow an easier detection of suspicious activities and allows to decrease the number of transactions which would not have been considered as suspect in isolation. This method provides a comparison between sequences and historical information. By this way, the detection of suspicious transaction can be performed according to its own trend which reduces the number of false positive and negative consequent to human-set threshold.

D) The Use of Visualisation Tools

As already mentioned in section 2.2, most of currently used AML solutions use predefined rules. These rules can be seen as a list of keywords based on predefined

patterns. In the purpose to provide an accurate detection, [7] presents, in addition to the classification, a visualization system.

This visualization system includes four tightly coordinated views of transaction activity; (1) The keyword network view, (2) The heatmap view, (3) the search by example tools and (4) a new visualization called StringBeads. Before any analysis or visualization, data are grouped according the sending and receiving accounts and visualizations use accounts instead of each individual transaction. In view of the enormous amount of accounts, a clustering of those ones is needed. This clustering groups accounts based on frequency of keywords that occurs in the transactions of the account.

The figure 2.4 shows the entire system with the heatmap(top left), search by example (top right), keyword graph (lower right), and strings and beads (lower left). The keyword network view represents the relation between keywords by means of a simple network graph. Keywords are related if they appear together in the same transaction. The heatmap view shows the relationship between accounts and keywords. The search by example tool allows to discover accounts of similar activities using some prototypes created on the discovering of previous results. Finally, the Stringbeads visualization depicts transaction over time.

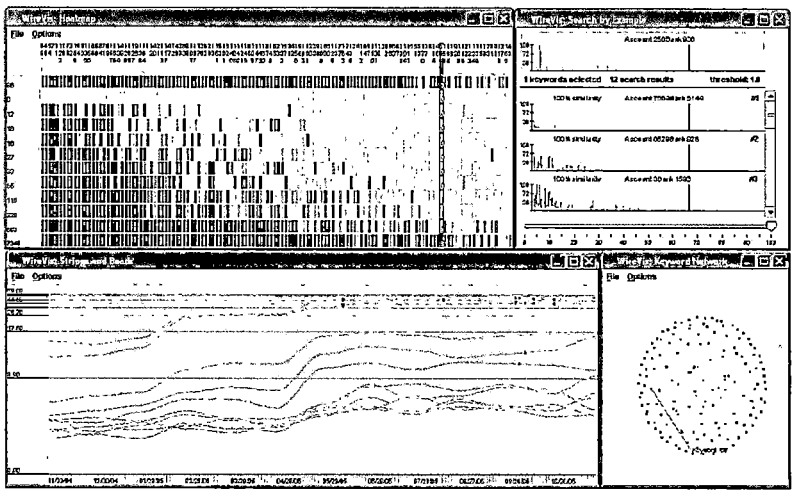

Figure 2.4: WireVis [7]

In sum, by this way, predefined keywords are used but supported by visualization tools which highlight relationships between keywords, between keywords and

account, which discover accounts with similar characteristics in the purpose to discover other suspicious accounts. This mechanism brings additional knowledge which can provide a more accurate future detection.

E) The Use of Algorithms which Calculate the Degree of Suspicion of a Person and the Degree of Association between two Entities

In section 2.2 about currently implemented AML solutions we have discovered that link analysis tools are already proposed to highlight the relationship between data. But these solutions provide only visualization tools and not really a data analysis.

The article [8] proposes a new method to detect the relation between data. In this method the degree of suspicion of a person and the degree of association between two entities are calculated via algorithms applied for each family or colleague members in cluster. By this mean, criminal networks could be identified and the classification can be more accurate.

Figure 2.5 illustrates this method. Four components constitute the system; an event-based database for criminal records, Data Preprocessing for criminal detection, Clusters and association detection, and visualization.

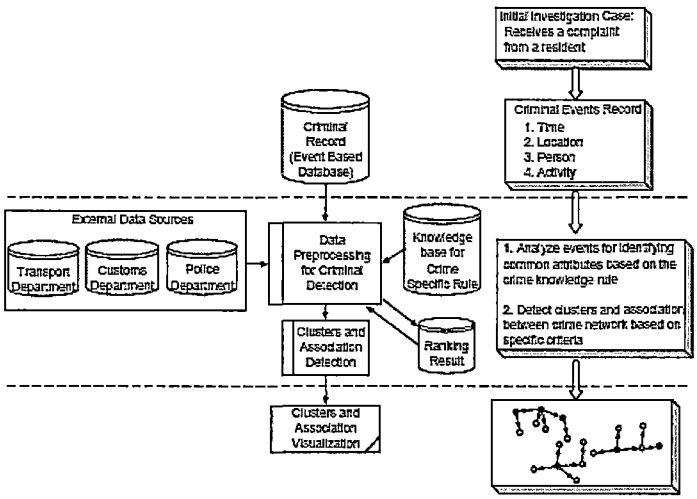

Figure 2.5: System design [8]

First, criminal information is stored in the database as objects with attributes (time, location...). An association between two objects represents a link between two

criminal entities. Money laundering occurring all around the world presents common characteristics. Data preprocessing in this model use a knowledge base to store crime specific heuristics. Criminal associations are identified based via the following attributes: Corruption Network (suspects use a network of trusted persons), Crime period (when the suspect is appointed as a key officer), bank transactions (frequent deposits...), suspicious entities (use of anonymous companies...), suspicious regions, suspect's career, suspect's age, suspect's salary, transaction behavior (number of transactions, type of transactions...).

In this method the degree of suspicion of a person and the degree of association between two entities are calculated via algorithms applied for each family or colleague members in cluster. The degree of association between two people is higher if two people have the same properties or are parts of the same transactions. The degree of suspicion is established by a score. The tables 2.6 and 2.7 respectively summarize the algorithms and the scoring scheme.

	Summary
Algo. 1	Identifies the family members of the suspect during a given period.
Algo. 2	Identifies the colleagues of the suspect during a given period.
Algo. 3	Calculates the degree of suspicion of the suspect and its colleagues within the cluster based on the type/nature of occupations.
Algo. 4	Calculates the degree of suspicion of the suspect and its colleagues/family members within the cluster. In this algorithm, bank transactions between the suspect and its colleagues/family members are used for calculation.
Algo. 5	Calculates the degree of suspicion of all members within the cluster based on the members' bank activities.
Algo. 6	Calculates the degree of suspicion of all members within the cluster based on the existence of shell companies.
Algo. 7	Calculates the degree of association between two entities.

Figure 2.6: Algorithms [8]

Condition	Point(s)	Apply to Algorithm
Degree of suspicion		
Family member of the suspect	1	1
Head of finance related department	1	3
Staff member of department under investigation (suspicious department)	2	3
Head of department under investigation (suspicious department)	3	3
Transaction between suspects' bank accounts	2	4
Large bank transactions	1	5
Degree of association		
Colleague association	1	7
Family association	2	7
Bank activity association	2	7

Figure 2.7: Degree of suspicion and association [8]

2.3.3 The Need to Have a System which can Use Different Database Format

Currently, provided AML solutions require a specific database format.

To solve this problem we can take a leaf out of the business intelligence:

In Business Intelligence (BI) the three-tier architecture is often used to place an interface between databases with different format and the used BI application. The different used databases have a different format (perhaps imposed by anoher application of by a law for example). In the purpose to be used with the application and its format requirements, a datawarehouse is created with the suitable format. By this way, the BI application can use this formated datawarehouse.

This method can be used to solve this problem. Between the detection application and the database of financial instutions, a formated datawarehouse can be created. The data from financial institutions will be extracted and loaded in a datawarehouse which will be used by the detection system.

Note that this three-tiers architecture and above all the use of a datawarehouse are confronted to some limits. Indeed needing an exportation, transformation and loading, the data are not available in real time in the datawarehouse. This can be a serious problem for our domain.

A community is today responsible to solve this problem of real-time and their results could be used to solve our problem.

2.4 Conclusion of The Technical Part

In the aim to identify the sources for the lack of efficiency of the ML detection performed by financial institutions, three levels have been analyses 1.3 : the technical, formal and informal levels.

This chapter analyses the technical level and highlights the reasons for the lack of efficient in the ML detection which can come from implemented AML softwares.

Even if the currently proposed solutions are already efficient if they are correctly used, interviewed experts highlight some limits which can be solved to improve the performance of AML systems. These limits, presented in section 2.2 are the following ones: (1) a lack of learning based on previous detection performed by human experts, (2) a specific database format required, (3) a configuration which is difficult, and (4) too much errors in the detection (too much false positive and false negative suspicious cases).

These limits reflect some additional important qualities required for a more efficient AML solution which would be more suitable for the ill-structured, changeable and complex ML and financial systems.

These technical requirements are the following ones: (1) adding a learning capability to AML systems, (2) adding mechanisms which can bring a more accurate detection, and (3) the need to have a system which can use different database format.

Concerning the difficulties to configure systems, a solution could be bring in each financial institution at informal level (see chapter 4.

A future work (see section 6.2) could have the aim to enrich these required qualities through additional researches in the literature and some meeting with experts in this field. Nevertheless, even if this list of requirements is currently not exhaustive, it brings some important indications to improve the efficiency of AML solutions.

Section 2.3 presents some techniques which can provide these required qualities.

In the purpose to provide a learning capability to solutions based on data-mining techniques, knowledge repositories and neural network can be used. The results of previous detection (the final decision, taken by human experts, based on potentially suspicious cases provided by the system) are stored in knowledge repositories. This knowledge is used to link a degree of suspicion for some kind of transactions. This calculation is used by a neural network to establish a ranking of detected transactions.

The learning capability can be provided by a solution which uses intelligent agents for the investigation. By their own properties, intelligent agents bring learnability by memorizing their anterior experience and their reasinning capability. Moreover, in collaboration with other agents, they can share knowledge they don't have in isolation.

In the purpose to provide a more accurate detection with less false positive and negative suspicious cases, some mechanisms can be used to improve the classification.

First, the use of leaning capability can provide an accurate classification thanks to the additional knowledge they bring based on previous detections.

Next, the use of a local outlier factor algorithm can measure the deviant degree of point of the category representing an abnormal behavior and points from the category representing a normal behavior. By this way, how the transaction is suspicious is then available and points in the abnormal behavior category can be ranked according their degree of suspicion.

Thirdly, a sequence matching can also decrease the number of errors in the classification. Indeed, a transaction can be considered as non-suspicious in isolation but can be suspicious if we analyse the history of an account and if we take into account transactions information.

The use of visualization tools to support the classification based on predefined keywords can also be useful to provide an accurate classification. Indeed, the visualization can highlight relationship between keywords, between keywords and account,

and can discover accounts with similar characteristics in the purpose to discover other suspicious accounts. This mechanism brings additional knowledge which can provide a more accurate future detection.

Finally, algorithms which calculate the degree of suspicion of a person and the degree of association between two entities can also be useful to provide a better detection which can be based on the identification of criminal networks.

To respond to the problem of systems which require a specific database format, a solution can be found through the three-tiers architecture which provides a kind of interface between datasets of financial institutions and AML softwares. This solution still presents some limits which are currently taken into account by all a community. The result of this research can help to solve our problem.

Chapter 3

The Formal AML System

The TFI model, presented on the section 1.3, proposes three systems evolving in the global AML information system: the technical, the formal and the informal AML systems.

After the technical AML system presentation in chapter 2, the current one deals with the formal AML system.

A formal system concerns attributes of the system which are documented and formalized in rules, procedures, etc. In the field of AML, a hierarchy among organizations formulating these rules can be identified [5]: trans-national organizations (e.g. the Financial Action Task Force (FATF)), national organizations (e.g. the regulators) and local organizations (e.g. banks). Local organizations establish their own internal policies based on the interpretation of trans-national recommendations by national regulators according to their own national priorities.

These three layers are presented in turn in the three first sections of this chapter. Then, some conclusions are drawn regarding the formal level.

3.1 The Trans-national Level

"Various international organizations are aware that money laundering and terrorist financing can greatly influence the global economy and the financial markets. That is why they have set up awareness-raising programs and urge political decision makers to take measures to counter criminals and terrorism financiers and to prevent

that they could take full use of the proceeds of their criminal activities or for terrorist financing purposes"' [35]. These international organizations are the FATF, the Egmont group, the European Union, the council of Europe, the UN, the IMF World Bank and the OECD.

This section presents these international organizations which takes all actions to fight against money laundering. The FATF, the Egmont group, the council of Europe, the UN, the IMF World Bank and the OECD have no formal authority and only provides recommendations, guidelines, forum, and help to governments to fight against money laundering. Only the European Union publishes directives which have a formal authority. Moreover, the actions of the Egmont group, the European Union, the council of Europe, the UN, the IMF World Bank and the OECD are all based on the FATF recommendations which are considered as standards in this field.

3.1.1 The FATF

In the late 1980s the Financial Action Task Force (FATF) is founded by the G7 group in an international effort to fight against money laundering. Currently, 29 countries and two international organizations (the European Commission and Gulf Cooperation Council) compose the FATF body [4].

In 1990, this independent inter-governmental entity which develops policies to fight against "money Laundering, financial terrorism and proliferation of weapons of mass destruction" published 40 recommendations first to fight the usage of the financial system for drug traffic [3]. These recommendations are grouped into 3 categories: legal measures (how legislative organs have to create a complete legal structure to fight), financial regulations (how governments should regulate their financial system) and international cooperation (how governments have to work together). The official FATF website notices that 8 new special recommendations had been added about financial terrorism after 11th September 2001 [37]. These new recommendations contain a set of measures to fight terrorism acts and organizations. These recommendations can be categorized in 3 groups [13]: (1) Requirements about client knowledge (KYC-Know your client)."*KYC guidelines require or recommend*

developing a keen understanding, through appropriate due diligence, of who the true beneficial owners and parties to transactions are, the source and intended use of funds, and the appropriateness and reasonableness of the business activity and pattern of transactions in the context of business" [13] (IFAC,2002). (2) Requirements about suspicious activity reports (SAR) and (3) Requirements including antiterrorism (AT) in AML.

Money Laundering can lead to destabilize the world economy but also implied other risks to which financial institutions are confronted like reputation risk, operational risk, concentration risk and legal risk [20]. It's the reason why FATF invites all governments and financial regulators to take necessary measures (process and procedures) to fight with efficiency against money laundering, the financing of terrorism and against other illicit activities [31, 20]. Currently, 180 governments have adopted FATF recommendations and require all their financial institutions to "indentify, track, and in some sense control terrorist funds - not only by blocking assets but also through stronger measures such as identity verification at account opening via government-supplied lists, and attention to the ongoing uses as well as the sources of funds" [13].

It's important to notice that "the FATF recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard" [11]. This is this status of standard which conducts authors of the literature to consider the FATF as the only one entity responsible of recommendations formulation at the international.

The FATF have also a role of evaluator [35]. Indeed, some members of the FATF participate with other experts to the evaluation of states concerning the AML. Once this evaluation performed, the FATF gives some recommendations to improve the efficiency of the detection.

3.1.2 The Egmont Group

A second entity at the trans-national level is the Egmont group of Financial Intelligence Units (FIUs). "In 1995, a group of FIUs met at the Egmont Arenberg Palace in Brussels and decided to establish an informal group for the stimulation of international co-operation. Now, known as the Egmont Group of Financial Intelligence Units, these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise.

The goal of the Egmont Group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field. This support expands and systematizes international cooperation in the reciprocal exchange of information, increases the effectiveness of FIUs by offering training and promoting personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs, fosters better and secure communication among FIUs through the application of technology, such as the Egmont Secure Web (ESW), also fosters increased coordination and support among the operational divisions of member FIUs, promotes the operational autonomy of FIUs and finally also promotes the establishment of FIUs in conjunction with jurisdictions with an AML/CFT program in place, or in areas with a program in the early stages of development" [41].

This group has no formal authority and only provides support and encouragements for a better cooperation and recommendations integration. For this reason, the Egmont group of Financial Intelligence Units is not considered as a responsible in the formulation of AML recommendations.

It's important to notice that actions of the Egmont group is destined to governments and not to private institutions and individuals [28].

3.1.3 European Union

"Since the nineties various measures to combat money laundering and terrorism financing have been taken at European level. The most important achievements are (1) various directives combating money laundering and terrorist financing were

adopted. The most recent one is the third directive (2005/60/EC), (2) Regulation 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community was adopted, (4) a Committee on the Prevention of Money Laundering and Terrorist Financing was created, in which CTIF-CFI and CBFA actively participate, to examine the technical implementing measures of Directive 2005/60/EC, (5) a discussion forum for financial intelligence units was created, the "Financial Intelligence Units platform". This forum discusses various aspects such as technical aspects for transposing the third directive, harmonizing of the approach of financial intelligence units, data protection and confidentiality, harmonization of databases, content of disclosures, disclosures of cash and cooperation between FIUs at European level, (6) a secure computer network, called the FIU.NET, was set up to exchange information between Member State FIUs." [35]

In the purpose to better understand the content of the directives, the description of the content of the Directive 2005/60/EC is proposed [29]. It's important to notice that these directives are based on the FATF recommendations recognized as an international standard and have to be applied in all member states.

The Directive 2005/60/EC describes in its first chapter the money laundering (art.1), who is concerned by this directive (art.2) and proposes some definitions of the used terms (credit institutions, financial institutions, property, criminal activity, serious crimes, beneficial owner, trust and company service providers, politically exposed persons, business relationship and shell banks (art.3). The chapter 2 concerns customer due diligence. This chapter describes in which cases states have to take measures in this field (art.7), what measures have to comprise (art.8) which are the obligations of states in this field (art. 9-10), which institutions haven't the obligation to apply this customer due diligence (art.11), etc. The chapter 3 describes the reporting obligations of states. The chapter 4 concerns the information and statistical data that states have to perform and record. In the chapter 5, the enforcement measures are described. These measures concerns as well Internal procedures, training and feedback, as supervision, cooperation or penalties [29].

3.1.4 The Council of Europe

"The Council of Europe adopted the Strasbourg Convention of 8 November 1990 on laundering, search, seizure and confiscation of the proceeds of crime.

Within the framework of the Council of Europe the evaluation program on anti-money laundering measures (PC-R-EV, a select committee of experts in charge of evaluating measures on fighting money laundering and recently renamed Moneyval) started in 1997. Moneyval is a FATF-style regional body that analyses the compliance with the FATF-Recommendations by its 25 member states (members of the Council of Europe with the exception of the FATF member states).

In 2008 the convention of 1990 was broadened to include terrorist financing given that financing can not only take place through money laundering but also through legal activities. The Council of Europe provides technical assistance to its member states in order to strengthen their ability to address money laundering risks." [35]

3.1.5 The UN

"The Vienna Convention of 20 December 1988 against Illicit Traffic in Narcotic Drugs and Psychotropic Substances was the first contribution of the United Nations (UN) to the fight against money laundering. It incriminated the laundering of the proceeds from drug trafficking.

In 1997 the United Nations Office on Drugs and Crime (UNODC) adopted the Global Program against Money Laundering (GPML) in view of stimulating the legal, administrative and judicial implementation of anti-money laundering mechanisms. It also created the United Nations Offshore Forum that urges the countries and territories concerned to observe the international criteria on financial regulation and money laundering when they provide international financial services.

On 14 December 2000 the UN adopted the Convention on Transnational Organized Crime that incriminates money laundering and contains measures on preventing use of certain sectors for money laundering purposes.

The United Nations is also involved in combating terrorism and terrorist financing. Since its creation multilateral disarmament and arms limitation are the main

goals in efforts to maintain peace and international security. The organization's main goals are to reduce and then eliminate nuclear weapons, destroy chemical weapons and strengthen bans on biological weapons.

Using resolutions 1373 (2001) and 1624 (2005) the Counter-Terrorism Committee aims at strengthening the capacity of Member States of the United Nations to prevent any terrorist acts on their territory or beyond [35, 42]"

3.1.6 IMF and World Bank

"Since 2001, the International Monetary Fund (IMF) and the World Bank (WB) have increased their involvement in the efforts against money laundering and the financing of terrorism, including strengthening their cooperation with the Financial Action Task Force (FATF).

In 2002 the IMF, WB and FATF jointly undertook the drafting of a comprehensive methodology paper in view of evaluating all countries worldwide against the international standards on preventing money laundering.

The IMF and WB also created a coordination mechanism for providing technical assistance to countries in view of strengthening their economic, financial and legal framework in the fight against money laundering and terrorist financing" [35].

It's important to notice that actions of this group is destined to governments and top banks and not to little financial institutions or individuals [28].

3.1.7 The OCDE

"The Organization for Economic Co-operation and Development (OECD) is based in Paris and has 34 members. Its mission is to promote policies that will improve the economic and social well-being of people around the world.

The OECD has several activities including:

- measuring productivity and global flows of trade and investment;

- predicting future trends;

- setting international standards on a wide range of topics, ranging from agriculture and tax to the safety of chemicals;

- organizing forums on various themes.

The fight against terrorism, tax dodgers, crooked businessmen and others whose actions undermine a fair and open society are amongst the themes discussed.

In 2011 the OECD organized a first forum on "Tax and Crime - A whole of Government approach to fighting financial crime" in Oslo, Norway."[35].

3.1.8 In Sum

In sum, at the trans-national level of the formal AML system, seven entities are present; the FATF, the Egmont group, the European union, the council of Europe, the UN, the IMF and World Bank, and the OECD.

The FATF recommendations recognized as the international standards for the AML and the financing of terrorism, are used by some other entities to provide forum, guidelines of cooperation, coordination mechanism, programs to stimulate the AML, evaluation program, etc., but also to provide resolution and directive which have formal authority.

The actions of these trans-national entities are principally destined to governments and some to top banks. In this level no measures are provided for smaller financial institutions and individuals.

3.2 The National Level

At the national level, international recommendations and directives which have formal authority are interpreted according to each respective national priorities. Therefore, all countries applying the same trans-national recommendations have their own AML organizational systems and different national laws are implemented in each country based on their recommendations interpretation. The success of the implementation of these recommendations depends on the strictness and the means of this interpretation [5, 22].

To illustrate this section, I propose to present the Belgian preventive anti-money

laundering and counter-terrorist financing (AML/CFT) system.

In Belgium, the National Bank of Belgium is today "responsible for the individual prudential supervision of the majority of financial institutions (micro-prudential supervision)" [34]. Each Belgian institutions involved in the AML process (see section 3.3) have to report their suspicions to the Belgian Financial Intelligence Processing Unit (CTIF-CFI). "The Belgian Financial Intelligence Processing Unit (CTIF-CFI), established by the Law of 11 January 1993, is a central part of the Belgian AML/CFT system.

CTIF-CFI is an independent administrative authority with legal personality and is supervised by the Ministers of Justice and Finance. It is led by a magistrate Mr. Jean-Claude DELEPIERE and composed of legal and financial experts and a senior officer seconded from the federal police. Its composition, organization, operation and independence are stipulated in the Royal Decree of 11 June 1993. CTIF-CFI is in charge of processing suspicious financial facts and transactions linked to money laundering and terrorism financing and are reported by institutions and individuals specified in the law" [35].

"The Law of 11 January 1993 applies Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as well as Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis. This law supplements the repressive approach to money laundering (Article 505 of the Penal Code) with a series of preventive measures carrying administrative sanctions and imposing on the specified institutions and individuals a duty to cooperate to detect suspicious transactions and facts and report them to an authority created for this purpose, the Financial Intelligence Processing Unit (CTIF-CFI)".

This law [1] describes who are the targets of this law (who has an obligations to report suspicious cases)(art. 1 to 6), in which cases these institutions and individuals have to identify their clients of the beneficiaries of their clients (art. 7 to 11), which are the actions that financial institutions and individuals described at the articles 1-6 have to perform and in which cases (art. 13 to 19), describes in which cases the payment in cash is limited (art.20 and 21), expresses in which cases and when institutions have the obligations to report suspicions to and collaborate with the CTIF-CFI, the obligations of the members of the CTIF-CFI, and other entities implicated in the transmission of information concerning money laundering of financial terrorism (art. 22 to 39) and finally sanctions if institutions and individuals concerned by the art. 1 to 6 don't respect their obligations.

3.2.1 Conclusion of the International and National Level

All states having "diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter ML" [11]. Even if the FATF recommendations "set an international standard, which countries should implement through measures adapted to their particular circumstances"[11], and even if these recommendations are recognized as the international standard in this field, they have not a real formal authority. Consequently, even if countries have endorsed these recommendations they stay free to establish their law and to interpret these recommendations how they want, with the strictness they want and according their interests and priorities. To help a most efficient as possible interpretation of international recommendations and directives at the national level some suggestions, guidelines, technical assistance, forum, etc. are established by trans-national entities (section 3.1).

3.3 The Local Level

The local level corresponds to all institutions and individuals involved in the AML process. To illustrate, as described by the article 2 and 3 of the Belgian Law of 11 January 1993 [1] cited in [35], the reporting obligation is applied to the following

financial institutions and individuals: the National Bank of Belgium, the Public Trustee Office, the Postal Service for its financial postal services, credit institutions governed by Belgian law, clearing institutions, payment institutions, intermediaries in banking and investment services, insurance companies situated in Belgium and authorized to deal in life insurance, insurance intermediaries, companies governed by Belgian law whose activities consist in giving investment advice or carrying out investment activities, the branches in Belgium of investment firms, collective investment undertakings governed by Belgian law, management companies of collective investment undertakings governed by Belgian law, the branches in Belgium of management companies of collective investment undertakings, persons situated in Belgium who professionally engage in transactions, mortgage companies situated in Belgium, market operators organizing the Belgian regulated markets, the natural or legal persons, the natural or legal persons that issue or manage credit cards, lease-financing companies, security companies that provide services of surveillance and protection for transporting valuables, dealers in diamonds. Moreover, this reporting obligation also implied professions as notaries, bailiffs, natural or legal persons that carry out activities in Belgium and are registered in the capacity of company auditor in the public register of the Institute of Company Auditors (Institut des rviseurs d'entreprises/Instituut van de Bedrijfsrevisoren), natural or legal persons entered in the register of external accountants and in the register of external tax advisors, natural or legal persons registered on the roll of approved accountants and on the roll of approved tax specialist-accountants, lawyers when they assist their client in the planning or execution of transactions concerning the buying and selling of real property or business entities; management of his money, securities or other assets, opening or management of bank, savings or securities accounts, organization of contributions necessary for the creation, operation or management of companies, creation, operation or management of companies, trusts, fiduciaries or similar legal arrangements, or when they act on behalf of and for their client in any financial or real property transaction.

All these institutions and individuals, referred in this work as "financial insti-

tutions" have a role in the ML detection. They are responsible for the detection and reporting of suspicious activities (as defined by the national level) [5]. These regulated institutions have to translate national laws and directives fighting against money laundering in detection procedures. They are also responsible to keep customer record, report large-value and suspicious activity reports and to coordinate with supervision centers to combat ML [22].

The ML detection process performed by financial institutions may be different according to the nature of the activities of the institutions and the country where it is established. For example, in Europe, as explained in subsection 3.1.3, the FATF recommendations are used by the European Union to establish directives imposing to all member states to establish laws to fight against ML. Each state publishes laws (e.g. the law of 11 January 1993 in Belgium described in section 3.2) requiring all financial institutions and individuals targeted by the European directives to implement measures according some cases and to report suspicions. The implementation of such measures, procedures is left to the responsibility of the institutions.

Consequently, sophisticated technical AML solutions are more or less used by financial institutions according the nature of their activities, their motivation, their attitude towards money laundering, etc.(see chapter 4). For example, the detection process in an institution which is principally implicated in the private banking will be different than the detection performed in a bank more active in the retail banking [26]. Let us discuss both of them.

The private banking is a service reserved to the richest customers. An institution which performs this activity knows well its customers and establishes a profile/scenario for each of its customers at the opening of each account. Through this profile customer information, profession, hobbies, habits, etc. are recorded. Moreover, the number of customer is limited and the amount on each account can be really high. For this kind of institutions, the ML detection in principally manually performed by AML experts. They compare a transaction which could be suspect to the initial profile established for each customer at the opening of each account.

If the potentially suspect transaction is not conform to this profile, therefore the transaction is considered as suspect and reported. The role of AML software's is only to help human expert to easily detect potentially suspect transactions in filtering some transactions according to the risky countries of people list for example. Highly sophisticated software's are not really useful due to the major place taken by the human analysis. The amount of money of a transaction is not a major indicator for such activity because it's a habit to see transactions with high amounts.

In the case of retail banking which is not a privileged service and which is accessible by everyone who wants to have an account into a bank, the AML process is different. The institutions don't know all their customers because the number is too large and no profiling is performed at the opening of the account. Only a general profiling for customers of the same kind is established. Moreover, the amount on accounts and the amount of transactions are lower than in the private banking. Therefore, the ML detection is different. This one is less case by case according a particular profile but performed by the software according to a general profile. The amount of transactions is more taken into account than in the private banking because a transaction of a high amount is not a habit. Therefore, in those institutions AML software's take a major place in view of the large amount of data and the quality and the level of sophistication of those systems is important [26].

In sum, the ML detection at the local level involves the translation of laws into procedures and measures in each institution and the reporting of suspect transaction to supervision centers. These procedures and measures are different among institutions according the nature of their activities. The success of the ML detection is linked to the strictness of the translation of laws into the institutions which is directly linked to the motivation to efficiently detect and report suspicious transactions, the attitude of the institutions towards anti-money laundering and the investment in this track (see section 4).

3.4 Conclusion of the Formal Part

To conclude this chapter, from the above we can easily understand that the formal AML system includes many actors at different levels.

As described by the section 3.1, the trans-national level involves seven entities invested in the money laundering and financing of terrorism problems. These entities are the FATF, the Egmont group, the European Union, the council of Europe, the UN, the IMF World Bank and the OECD.

These entities provide forum, guidelines of cooperation, coordination mechanism, programs to stimulate the AML, evaluation program, etc., but also resolutions and directives which have formal authority. These actions, which are mostly destined to government and top banks, are based on the FATF recommendations recognized as the international standards for the AML and the financing of terrorism.

At the national level, directives and resolutions with formal authorities taken by international entities based on the FATF recommendations are interpreted according countries'priorities, financial system, legal structure, etc.. Help is provided by international entities which provide forum, guidelines, motivate collaboration, etc, but this interpretation stay under the responsibility of each country and only the final result at the local level is evaluated.

At the local level, AML national laws have to be translated into procedures and measures according to the nature of the activities of institutions. These procedures and measures are applied in financial institutions to detect money laundering as best as possible. To perform this detection, sophisticated AML software's can be more or less useful according to the nature of the activities of institutions. Indeed for some kind of activity (e.g. the private banking), the human analysis take a bigger place than technical AML solutions. In the opposite, for other activities (e.g. the retail banking) sophisticated AML solutions take the major place in the ML detection.

Therefore, at the formal level, the success of the detection of suspicious activities firstly depends on the interpretation and the implementation of trans-national recommendations into laws at the national level. In this level, a lack of performance in the ML detection could be explained by a bad interpretation of recommendations into national laws. This could reside in the fact that some countries don't use guidelines, forum, help, etc. proposed by the international entities (see section 3.1). Moreover this interpretation is linked to national priorities, financial and legal structure of each country. Perhaps that the detection of money laundering is no the first priority for all countries and that all countries are not motivated in a same level by a strict and efficient interpretation of international recommendations.

Lastly, the success also depends on the translation of these national laws into procedures and measures into financial institutions, at the local level. The success of the ML detection in this level is linked to the strictness of this translation and to the motivation to efficiently detect and report suspicious transactions. Whatever the taken measures and used tools, the success of the ML detection highly depends on the motivation, and implication of the institutions, this will be discussed in chapter 4.

Chapter 4

The Informal AML System

4.1 The analysis

As explained in chapter 3, the gap between institutions which are efficient in the ML detection and those ones which are less is linked to the right translation of national laws into procedures and measures and their good applications by financial institutions.

This chapter analyses the main factors influencing the performance of the translation of law into local procedures and therefore also influencing the ML detection performed by financial institutions. To this purpose, the third and less embedded system of the AML information system presented by the TFI model (section 1.3) - the informal AML system - is then presented. This system consists in the attitude, culture, beliefs, motivation and implication towards the ML problem.

This chapter is based on two surveys, one [5] among 30 London banks and another [22] among Chinese financial institutions, and on two interviews: one [26] of a Belgian compliance officer in a private Belgian bank and the other [28] of a AML specialist who has worked in the AML sector in different countries and which supervises the ACAMS, Association of Certified Anti Money Laundering Specialists.

4.1.1 Two Surveys

Xuan and Pengzhu [5] relate a survey of 30 London banks performing interviews of ML reporting officers (responsible for ML detection in financial institutions). This survey examines the attitude toward ML controls, the beliefs about the efficiency of ML regulations and about the performance of technical ML solutions.

It reveals that "27 percent had a positive attitude towards ML controls, 40 percent were neutral and 33 percent had a negative attitude. In addition, 60 percent believed that ML regulations were ineffective in reducing ML, and it was felt that the costs largely exceeded any benefits. Larger banks tended to have more positive attitude towards ML monitoring than median and smaller ones, and than wholesale banks in general.[...] Where the Money Laundering reporting Officer is an senior manager, with direct access to the management board, it is easier to obtain resources and recommendations are likely to be acted upon more quickly"[5].

In another survey, Liu and Zhang [22] translate words from Chinese commercial banks and explain that "commercial banks sometimes regard AML as a kind of time-wasting and money-consuming job". They add that these commercial banks consider that "AML cannot bring direct profits but bring high costs" and that " AML in financial institutions can be viewed as a kind of risk management; Failure to report Suspicious Activity Reports (SARs) will enhance the compliance risk, sometimes influence the bank's reputation and finally transferred to be a commercial risk". Some managers consider that AML management could "drive customers away from banks because customers always search for financial service with simple procedure, high quality guarantee of business secret... complex investigation required by AML governing agencies scares customers away..."

These words are approved through the survey of London banks [5] where they find the same opinions among managers. They reveal that "some banks adjust models' parameters in order to reduce the number of alerts that they need to investigate". They add that "senior managers and staff see AML as a regulatory requirement and an administrative burden focused on avoiding sanctions". Moreover they point out

the "risk of damage to the banks' reputation".

4.1.2 Two Interviews

An interview of a compliance officer in a Belgian private bank [26] completes the view proposed in the two presented surveys with additional information particular to the private Belgium banking context. According to this person, in this institution, the person at the head of the compliance department is legally responsible of the ML detection. If a ML transaction is not detected the compliance officer can be pursued for complicity. Moreover a lack in the ML detection can conduct to a reputation risk for the institution. This legal responsibility and reputation risk increase the motivation of the ML department to perform the detection as well as possible.

This person adds that in this private bank, the detection is principally manually performed. It is based on a personal profile established for each customer at the opening of each account. The goal of this detection is principally the detection of the origin of funds. And it is preformed based on client justification and a check of this justification according to the initial customer established profile. The role of software in this detection is limited to the filtering of some transactions according some criteria but the major part of the analysis is performed by human experts. However, this officer plans to introduce a more sophisticated AML system not by conviction of its efficiency but more to show governement that sophisticated measures are taken to seriously fight against money laundering. Indeed, she thinks that this new solution cannot bring more that the already currently performed detection which is principally based on human analysis. Moreover, sophisticated AML systems are considered by this officer as a waste of time because they have to introduce manually all the rules they use in the system. Lastly, which finally provides too much false positive detected cases and a waste of time.

Another interview of a certified AML specialist [28], reveals that the most important lack of efficiency resides in the AML staff in financial institutions. Indeed, according this specialist, the majority of currently proposed AML solutions are ef-

ficient. The lack of efficiency is in the use of these tools.

The specialist assesses that most of compliance officers and AML staff don't know the ML process and the AML world. Moreover, these people are not always specialists in banking system but can be lawyers, etc. and therefore don't understand in details the complexity of the banking process. Consequently, confronted to technical AML systems they don't know what they are looking for, what they want from the system, they have difficulties to integrate efficient rules in the system which can conduct to an efficient detection. Moreover, most of financial institutions don't want to invest time in well understanding the software, its parameters, its options, etc. and therefore don't efficiently use it. In addition, they don't want to invest time in AML conferences, AML training, etc. to increase their knowledge in the ML process and in the detection. They buy a system to respect the law but don't use it with efficiency and are not invested in the ML track.

According this specialist, these problems are directly linked to the motivation and the moral responsibility in the ML track. Indeed, financial institutions have the choice between implementing measures which are sufficient to respect laws and implementing measures to really stop the money laundering and to be active in this track.

4.2 Conclusion

Through these interviews and surveys, several issues of the ML detection from the informal level can be highlighted.

As already explained in previous chapter, the ML detection performed by financial institutions depends on the nature of their activities, their motivation and implication in the ML track. Consequently, the level of efficiency of the AML detection can differ among institutions.

This gab can be linked to different factors. They are presented below through three levels: the level of the organization itself, the senior management level, and the level of the AML staff/employees. At the level of the organization, the nature

and the attitude of organizations towards ML and the communication among them directly influence the efficiency of the detection. Secondly, the attitude of the senior manager is also linked to the implication and motivation in the ML track. And thirdly, the employee incapability and training inefficiency are also implied in the detection inefficiency.

4.2.1 The Organization

A) The Culture of the Organization

The culture of the organization has a real impact in the implication and the motivation for a ML track. Some companies speak about a "corporate social responsibility", a "moral responsibility towards the customer", "an ethical responsibility", etc.[5, 26]. The implication and the motivation for the ML track is highly linked to this ethic and moral responsibility which surpass the simple commercial and competitive goal that an institution can find in the AML track (see subsection 4.2.2).

The place that certain compliance officers allocate to the human analysis in the ML detection can influence the investment in costly and highly sophisticated AML software's. Indeed, for some compliance officer, the human expertise has the major place in the money laundering detection and the use of highly sophisticated AML software's is more considered as a waste of time [26].

B) The Attitude towards ML

The motivation for the implementation of a decision support system which efficiently tracks money laundering depends on the attitude towards money laundering [5]. Indeed, some commercial banks can see the track of money laundering as "a time-wasting and money-consuming job" [22]. Moreover, some consider the management of money laundering as having a negative impact on the relationship with customers and as a risk to lose those ones and therefore important business. A risk linked to the reputation is also highlighted; according to some managers "failure report SARs will enhance the compliance risk and influence the reputation".

The literature links this attitude with the size of institutions. Indeed, some

survey reveals that the attitude toward money laundering management is more positive for larger banks than smaller. A reason could be the larger amount of transactions of these banks which implied a higher risk on the world economy and for the institution itself.

C) The Lack of Communication between Institutions

Once an organization is implicated in the ML fight and has motivation enough to conduct this task as well as possible, other problems decreasing the efficiency of the detection can appear. A problem can come from the lack of communication between different institutions which not exchange information easily for strategic, legal and operational reasons. "Without appropriate sharing of information, it is extremely difficult to verify the effectiveness of the ML modeling exercise." It is also difficult to know which ones of those available systems are more efficient than others in the ML detection and therefore improving developped solutions [5]. Concerning the inter-institutions communication, it's important to take into account the data secrecy. Indeed each bank can only access to the data of its own customers and only to the account number, sometimes the name of a customer of another bank. Therefore, this communication and information sharing know important legal limitations [26].

4.2.2 The Senior Management

The attitude of the senior manager is also directly interrelated with the adoption of a more or less efficient and sophisticated AML solution. When the senior manager supports AML and is convinced by the efficiency and the usefulness of an AML solution for the organization, more budget will be available to implement a more efficient and more sophisticated, therefore more costly, ML detection software [5].

It's important to understand that the implication of senior management in the fight against money laundering is highly influenced by media attention. Indeed media can bring more or less attention on the implication of institutions in the fight against money laundering. This attention can create a real positive commercial return for those institutions. One reason why some senior managers are motivated by the implementation of a highly sophisticated and efficient solution could be to

send the message that the organization takes seriously into account the ML problem. Therefore, in this case, tracking suspicious activities has more things in common with a commercial and competitive goal than a real ethic implication.

Moreover if the AML responsible is a person who has access to the board, there will be more AML actions and implication from the organization[5].

4.2.3 The Employees - Capabilities and Training

Another reason for the lack of efficiency of the ML detection could be "the employee incapability and training inefficiency" [22] of some organizations. AML staffs are often not aware about the responsibility and the risk liked to money laundering management. They view AML as "a method to guard the finance order in their country" and therefore are not really implicated in this track and don't invest time to learn more, to follow conferences, to learn the system they use to improve its performance, etc.. Moreover compliance officers are not always specialists in the banking process and in AML. Therefore, they don't understand the ML process using the banking system. Consequently, they are not able to implement efficient rules in system which decrease AML solutions' performance.

Moreover, the survey [22] highlights that AML staff is instable. Indeed they follow training and one year later they are transferred in another department and other employees are trained. This instability obstructs a high AML expertise and experience by AML staff.

It also appears that trainings proposed by AML solutions providers only explain the system in general and are not really detailed and focused on the improvement of the ML detection. Moreover, they do not evolve with the evolution of the ML system and the content of these trainings is continuously the same one and not enough linked to the reality (no case, no application, and no detection example).

Chapter 5

Conclusions and Recommendations

As presented in section 1.3, the money laundering information system is composed of three independent and interrelated subsystems: the technical, the formal and the informal system. Current research about money laundering is mostly based on one of these three system: the technical articles presenting systems don't care about the legislation around money laundering, nor about the technical capabilities of AML staff in financial institutions, the legislation don't care about methods used by financial institutions to respect it, etc. This thesis aims to explain the reasons for the lack of efficiency in the ML detection performed by financial institutions in analysing the three systems. Thanks to this inter-domain analysis, a more complete and realistic view of the reasons for the lack of efficiency of the ML detection is provided.

Chapter 2 describes the technical system, highlights limits of currently implemented AML systems and proposes some techniques which could overcome these limits. The formal level is studied by chapter 3 and highlights issues for the ML detection at three levels: the trans-national, national and local level. Finally, chapter 4 explores the informal level and develops issues linked to the AML staff which decrease the efficiency of the ML detection in certain institutions.

The current chapter is divided in three sections: the technical level, the formal level and the informal level. For each section, firstly a summary is proposed and

next, recommendations for a better performance are exposed.

It's important to understand that due to the difficulties met to access implemented systems, the technical recommendations are conceptual and based on my intuition after the investigation of some articles of the literature about AML systems. Consequently a more deep and concrete investigation and meetings with solution users and providers could bring more detlailed and less intuitive recommendations at the technical level. Concerning recommendations at the formal and informal level, these ones are also based on gathered information and more interviews are also needed to provide more concrete and complete recommendations (see section 6.2).

5.1 The Technical Level

5.1.1 The Current Situation

For institutions with a large amount of customers and transactions, the use of AML technical systems takes a major place in the ML detection. Moreover, as presented in the TFI framework (section 1.3), this system is the most embedded in the global AML information system. This central position highlights the importance of this technical system but also the fact that this one is directly influenced by the two other systems: the formal and informal ones.

Section 2.2 presents limits of techniques involved in currently implemented AML software's highlighted by interviewed AML experts. This investigation has resulted, in section 2.2.2, in required qualities for a more suitable and efficient AML system. These requirements are the following ones: (1) adding a learning capability to AML system, (2) adding mechanisms which can bring an more accurate detection, and (3) the need to have a system which can use different database format.

For each of these expected qualities, some solutions are presented in section 2.3.

Knowledge repositories and neural network can be used to bring learning capabilities to data mining - based solutions. The results of previous detection are stored

in knowledge repositories which are used to link a degree of suspicious for some kind of transactions. This calculation is used by a neural network to establish a ranking of detected transactions.

Intelligent agents can also be used in AML solutions for the investigation. By their own properties, intelligent agents bring learnability by memorizing their anterior experience. Moreover, in collaboration with other agents, they can share knowledge they don't have in isolation.

In the purpose to provide a more accurate detection with less false positive and negative suspicious cases, some mechanisms can be used to improve the classification: (1) the use of learning capability bringing additional knowledge which can provide an accurate future detection, (2) the use of a local outlier factor algorithm which can rank abnormal transactions according their distance to the category of point with a normal behavior, (3) the use of account history and transactions information to see transactions as a temporal sequence and not more in isolation, (4) the use of visualization tools supporting the classification based on predefined keywords in highlighting relationships between keywords, between keywords and account, and can discover accounts with similar characteristics in the purpose to discover other suspicious accounts, and (5) the use of algorithms which calculate the degree of suspicion of a person and the degree of association between two entities to identify criminal networks.

Finally, implementing a three-tiers architecture can allow to respond to the problem of systems which require a specific database format in proposing an interface between datasets of financial institutions and the used AML software.

5.1.2 Recommendations

As summarized above, a more efficient AML solution would perform a classification with a minimum of errors based on predefined rules and on the results of previous detections.

Two kinds of solution are able to perform this detection: data mining-based

solutions, and intelligent agents-based solutions.

A) A Data-mining-based Solution

Data-mining methods are particularly suitable for the ML detection. Indeed some methods are descriptive and allow for example the classification, the identification of trends and correlations, the profiling of some customers, etc., while others are predictive and allow to predict new trends, patterns, etc. based on previous detections.

In the purpose to provide an accurate classification provided by DM tools as clustering it's more than required to add a learning capability. In this purpose, the storage of additional knowledge from previous detection in a knowledge repository can be a suitable solution. Techniques as neural networks can bring an accurate classification through a ranking of detected transactions based on previous detected ones stored in the repositories.

It's important to understand that this learning capability could be really useful in long term because as explained by a Belgian compliance officer [26], the amount of suspicious cases which are really detected and considered as suspect is so low (three last year for this officer) and have so little points in common that a learning will bring not really additional knowledge and will be not really useful for future detections in short term. Moreover an artificial/supervised learning is not really possible in the ML context due to the unpredictable aspect.

But it should be interesting if all detection cases from all banks of all countries could be put together to provide interesting additional knowledge useful in more short term.

Some additional tools evocated in section 2.3 also allows to increase the precision of the detection. These possibilities are the use of a local outlier factor algorithm, the use of a sequence matching, the use of visualization tools, and the use of algorithms which calculate the degree of suspicion of a person and the degree of association between two entities.

B) An Intelligent Agents-based Solution

A solution used intelligent agents is developed in section 2.3.1.

As defined by the French Normalization Association, an intelligent agent (IA) is "an object using artificial intelligence techniques: it adapts his behavior to its environment and acts as a learning sub-system by memorizing its anterior experience. It enriches the system it uses by adding automatic functions treating, controlling, memorizing and transferring information."

Properties of an IA are the following ones: an IA is autonomic, enable to communicate and cooperate, enable to reason and react to its environment and is mobile. It also includes one or more of the following elements: a predefined knowledge base, and an inference motor (which allows having complex reasoning). Moreover, it can also include a knowledge acquisition system and a learning mechanism [17]. A multi-agents system (MAS) is a group of agents which interact together in a specific environment to reach together their goals. They take other agents knowledge and capabilities to overcome their own limits [15].

At the section 2.3.1, these IAs are applied following Real-time Exception Management Decision Model which is a suitable model which imitates the decision process that a human would follow to detect ML cases. It's important to have an accurate detection to fit human decision in the ML world as well as possible. Indeed according to this model, the goal of each agent is defined.

Intelligent agents fit also perfectly the complex AML environment which involves many entities [13]. Indeed, agents could be autonomously and collaboratively responsible for different activities. An interesting point in using IAs is the fact that each agent having its own work, if we want add functionalities to the model, it's possible to add new agents and therefore redesign the model by simply adding new agents. Moreover, thanks to these properties, intelligent agents bring learning capabilities and adaptability which are completely suitable for the ML context.

C) Conclusion

In sum, through our investigation we can highlight two technical options: (1) using data-mining tools with natural computing techniques and additional tools to provide an accurate detection or (2) using a multi agents system following a good making decision model. Note that these options are not excusive.

These two options present advantages but also difficulties. The use of data-mining tools requires a suitable parameter selection to be really performing. In contrary, once build intelligent agents are performing and not depend on a parameter selection. But to be performing together, IAs have to follow a performing making decision model defining the role of each agents. Moreover intelligent agents don't need additional tools to provide the required learning capability which is a real advantage for this option. Another points in favor of the use of intelligent agents is the fact that if we want add functionalities to the model, it's possible to add new agents with a new work in the model and by its properties, these agents will automatically work with other ones already implemented in the model.

We can then notice that the use of intelligent agents for the ML detection can also be an option even if currently the most of proposed solutions are data-mining-based solution.

5.2 The Formal Level

5.2.1 The Current Situation

The formal level, presented in the chapter 3, concerns as well international recommendations and directives as the interpretation of those ones in laws at the nation level, but also the translation of laws into procedures and measures in the financial institutions.

At the trans-national level, the FATF formulates recommendations on which are based directives which have formal authorities (e.g. the directives of the European Union). Members of those entities have to interpret these directives and integrate it

in their laws at the national level. Other trans-national entities provide guidelines, suggestions, forum, technical assistance, evaluation, help, etc. to governments and top banks for a suitable interpretation of international directives in national laws.

At the local level, AML national laws are translated into concrete procedures and measures to detect and report ML according to the nature of the activities of institutions.

Therefore, at the formal level the success of the detection of suspicious activities depends first on the interpretation and the implementation of trans-national recommendations into laws at the national level and next to the right translation into procedures in each institution.

5.2.2 Recommendations

The lack of performance in the ML detection could reside in the fact that some countries don't use the help provided by international entities as forum, technical help, evaluation, etc. Moreover this interpretation is linked to national priorities of each country. Perhaps that the detection of money laundering is not the first priority for all countries.

In the purpose to improve the performance of the detection some measures can be taken at the trans-national level. Indeed, currently only guidelines are proposed to countries for the interpretation of trans-national recommendations in national laws but countries stay free to interpret these ones in a more or less strict way. To avoid not strict enough interpretations, it should be useful to legally impose some guidelines or to control the national laws to be sure that they are strict enough.

Next, the success also depends on the translation of national laws into procedures by financial institutions, at the local level. The strictness and rigor of this translation is directly linked to the level of motivation and implication in the ML track (see section 4.

The detection of suspicious behaviors depending on the nature of the activities of financial institutions, some guidelines/standards having formal authority have to

be implemented according this nature (e.g. for private banking, for retail banking, for lawyers, etc.). These guidelines with a formal authority as well for the interpretation of trans-national recommendations as for the translation of national laws into procedures could set a certain level of strictness which can also be controlled by international entities with a risk for the reputation of the institution in the case of a negative evaluation.

Another recommendation to motivate the rigor of the translation of national laws into procedures at the level of financial institutions should be, as already done in Belgium, to impute a legal responsibility to the person at the head of the compliance department of each institution integrated in the AML process. This legal responsibility can strongly motivate the entire AML track in financial institutions and can also increase the communication among compliance officers of different institutions about suspicious cases.

5.3 The Informal Level

5.3.1 The Current Situation

The section 4 has described problems meet at the informal level which can have a negative impact on the ML detection. These issues have been classify in three groups: these ones related to the institution itself (its nature, its attitude towards the AML track and the lack of communication among institutions), those linked to the senior management in these institutions, and issues at the level of employees (their incapability and the training inefficiency).

At the level of the organizations, the implication and the motivation for the ML track is highly linked to an ethic, a moral responsibility in the ML problem. Moreover, the place allocated to the human analysis can take in the ML detection can influence the investment in costly and highly sophisticated AML software's.

The attitude of institutions towards money laundering is also directly linked to the motivation for the implementation of efficient measures to track money laundering. Some institutions have a negative vision of the ML track and consider it as a

waste of time, as a risk for their reputation, a risk to lose important business, etc.

Finally a lack of communication among institutions has also been highlighted as a limit for an efficient detection.

At the level of the senior management, the attitude of the senior manager has an important impact in the implication of the institution in the ML detection. This motivation can come from a moral responsibility or from a commercial ambition.

Concerning the AML staff, some issues have also been highlighted:(1) the lack of knowledge in banking system and ML process of compliance officers and therefore an under-efficiently use of implemented technical solutions, (2) the lack of awareness and time investment concerning the ML process, the importance and impact of the detection and their responsibility in this process,(3) a training concerning the used AML system which is too general and not focused on the improvement of the ML detection according the nature of the institution and (4) the problem that in some institutions the AML staff changes too frequently.

5.3.2 Recommendations

In the purpose to increase the motivation for the ML track in institutions, a measure can be taken to increase the responsibility of person of the head of the compliance department. This person is as a cornerstone for the motivation and the implication of the AML staff in their job and is also responsible for the training, the AML awareness, etc.

In Belgium this responsibility is forced by a legal responsibility imposed to the person at the head of the compliance department in financial institutions. Perhaps that if such measures were introduced in other countries, the global ML detection which is an international process could be improved.

It's also important to have, as senior managers, people with an implication and a motivation for the AML track. An awareness person can allow more investment in this field, and can support the decision of the compliance officers.

Concerning the training and the awareness of the AML staff, several solutions are possible. First of all, to be efficient, it's necessary for institutions to have a dedicated AML staff which is not all the time transferred to another department. Next, the AML training and awareness could be enhanced by governments which could require that the AML staff follows certain AML conferences and workshops to better understand the AML world and the ML process. Secondly, compliance officers which have no formation in finance or experience in the banking system should have the obligation to follow formations in this field to better understand the banking system. Moreover, the training concerning the implemented AML system proposed by providers would be more specific to the nature of financial institutions and to the improvement of the ML detection according this nature.

Concerning the communication between institutions from a same country but also between different countries, it's important to understand that this communication is limited by the data protection imposed to the financial system. But establishing as in Belgium, an entity which is responsible to receive all suspicious cases from all institutions of a same country and which has access to all account information in the country can be useful to have a more global view and to be an intermediary for the communication among institutions.

Chapter 6

Methodology and Future Work

6.1 About the Methodology

This thesis is based as well on three interviews of experts in the field of money laundering as on the literature about money laundering at the financial, financial and governmental level.

This section describes these two ways of research and highlights some difficulties met in these investigations.

6.1.1 The Literature

In the purpose to understand experts'assertions about the lack of efficiency of the ML detection performed by financial institutions, a part of this research is based on article of the literature. This investigation is perfomed as well at the technical level describing techniques and mechanisms to fight against money laundering, as at the formal level with the investigation of international recommendations and directives, national laws, etc., and also at the informal level with surveys performing interview in some financial institutions about the motivation and the implication of the AML staff.

Concerning the technical literature a serious difficulty has been met. Each tech-

nical article presenting a new framework, algorithm or technique to better detect suspicious activities is oriented by the interest of its authors. Indeed, these articles are written by experts in specific technical domains: data-mining, intelligent agents, statistics, etc. who want to follow the AML stream which presents an increasing interest. In this purpose, they try to stick their own experience of their domain to the ML detection. They highlight some current AML solutions limits that their technique can solve and often don't discuss other limits that their solution cannot solve. The expectations for a new AML solution which could be more suitable and efficient than previous one, are sometimes too oriented and limited to what the techniques presented by authors can propose and solve. Identifying AML current solution limits and techniques which could overcome those ones is really difficult and requires a strong and long investigation.

Moreover, proposed technical solutions often forget constraints and limits linked to the financial system. These limits are as well legal constraints like the data protection as practical constraints like the content of a transaction which is principally no text but only account numbers, sometimes a name and a communication. For example a proposed technique is the use of keywords for the investigation while almost no text is present in transactions. Another example is the proposition to implement techniques highlighting relationships among accounts to identify criminal network. In theory this proposition will be useful but legally a financial institution only knows the details about accounts in its entity and only the number of account in other institutions. From the fact that the ML process implies many institutions, is almost impossible for an institution to identify relationship as family link, etc.

6.1.2 Interviews

This thesis involve three interviews, one of a detached expert at the internal affairs department at the European Commission, one of a person at the head of the compliance department in a Belgium Private Bank, and a third one of a person at the head of a large group of EU compliance officers and member of the ACAMS, the Association of Certified Anti Money Laundering Specialists.

Through these three interviews, I could have a first concrete and practical view of the AML process and perceive the complexity of this international process involving many entities at many levels in many countries.

I could also receive information which was really specific to the context of the interviewed person. For example, the person at the head of the compliance department in the Belgian private bank could bring me information specific to the AML process in a private bank in Belgium.

Consequently I could understand the importance to not only performing an investigation through the literature but also to increase the number of interviews. To have a total and concrete view of the AML process it is needed to interview as well all kinds of institutions and individuals targeted by the 2005/60/EC directives (see subsection 3.1.3 in different countries as members of the formal system (see section 3 at the international and national level in different countries.

This goal has been confronted to some difficulties linked to the sensitive aspect of the AML system. Indeed, it was really difficult to meet people in this field without knowing people who have contacts in this system.

Therefore this thesis is limited to a conceptual aspect with some limited practice and concrete elements which bring already serious indications, elements and hypotheses concerning the lack of efficiency but which could be more substantive with more meetings. This lack of interviews and access to implemented systems conduct to propose recommendations which are conceptual, intuitive and not enought detailed. Consequently more interviews at the formal and informal level, a more deep and concrete investigation, and meetings with solution users and providers could bring more detailed and less intuitive recommendations at the technical level, formal and informal level(see section 6.2).

6.2 Future work

As explained in the section 6.1, the current thesis already proposes a first and detailed view of the AML process and of some of sources of its lack of efficiency but is

limited. The proposed recommendations are also limited to conceptual and intuitive propositions. These limits are first due to the available literature in the technical area which is biaised and too oriented in the technical expertise domain of authors. Secondly, the sensitive aspect of this field obstructs the access to really implemented systems and contact with experts. Therefore this work is principally based on the literature about money laundering sustaining some experts' assertations.

My goal is to continue this work and to go beyond the presented limits of this thesis.

If this thesis is limited to the literature review it's principally due to difficulties to have appointments. For the moment I've only meet three really interesting experts in the AML domain. These people bring me a first contact with the real ML track and I could realize how much it's important to meet experts and to join the real AML world.

Therefore, I plan to continue this investigation and to meet other people from the AML system as well in Belgian institutions as in other countries. I plan to meet people from different areas: as well commercial, private, retail banks as international and national bank. I would like to have contact with those diverse domains of activities because the nature of those activities influences the methods taken to fight against money laundering in financial institutions. I would also meet the other institutions and individuals cited in the art.2 of the 2005/60/EC directive in different countries.

The limitations of this thesis conduct me to currently propose a conceptual work based on an inter-domain analysis which brings already serious indications, elements and hypotheses concerning the lack of efficiency in the ML detection performed by financial institutions but which is too conceptual and too far from the real AML system which is really complex. This work requires now an immersion in the real AML system to be more realistic, practical and less conceptual. It's the reason why I hope to have the chance to continue this work through a PhD.

My ambition is first the identification of the lack of efficiency through AML software's aiming to provide a better solution with new framework and more suitable

techniques. The current thesis identifies some limits through the literature and some techniques which can overcome these limits. But obviously it's only a conceptual and literature based analysis which has to be supported by a practical cases.

In this purpose, I plan to meet some AML solutions providers, discussing with them which techniques they use and the reason of their choice. Through these meetings I firstly want to compare the performance of the different implemented techniques. Secondly, I would like to discuss with technical expert about possible other techniques which could improve the efficiency of their solution.

Morover, many pieces of research are performed about the gap between business and IT in other domains. I could be interresting to indentify on which criteria they base their analysis. By this mean we could perform a similar investigation in the AML domains.

Next, I would like to catch information at the formal and informal level and about their influences on these AML technical solutions.

At the informal level, it appears that the efficiency of the ML detection depends on the implemented solution but not only. Indeed, two identical AML solutions implemented in two different institutions in a same country have not the same efficiency because the informal environment is different (e.g. due to the implication of the AML staff, the awareness of the senior management, the moral responsibility and ethic instead of a simple commercial goal...). It appears also that this informal environment is directly linked to the training for the AML staff which is not practical enough: no example enough, no application, etc. Therefore I would like to take contacts as well in commercial and non-commercial banks, national and international ones as public or private institutions. The major goal of this investigation would be to discover if there are differences of efficiency linked to something other than technical solution and directly related to the nature of the institution (private, public, commercial, non-commercial, etc). I'll analyze the level of motivation and implication in the AML process according the nature of the firm.

At the formal level, it appears that two identical solutions implemented in two different countries haven't the same efficiency. This is directly related to the interpretation of the trans-national recommendations (FATF and EC directives) by each

nation according to their own priorities and the translation of national laws into local procedures according the nature of the activities of financial institution. Then I would like to analyze firstly what is different between countries interpretation and which interpretation provides the more efficient ML detection, and secondly I would like analyze the translation of laws into procedures performed by institutions.

In the purpose to continue my investigation with a more concrete aspect and to provide a global view highlighting reasons for the lack of efficiency as well at the technical level as at the formal and informal ones, I've already take some contact with the European commission which have a role at the formal trans-national level, With the ACAMS, "THE international membership organization dedicated to enhancing the knowledge and expertise of AML/CTF and financial crime detection and prevention professionals, from a wide range of industries, in both the public and private sectors" [40]. I've also contact with the National bank of Belgium (BNB) which has the responsibility of the AML control, and with the bank international du Luxembourg and the bank Degroof. I've also a contact with SAS and the responsible of the compliance department at SWIFT, the Society for Worldwide Interbank Financial Telecommunication, "a member-owned cooperative through which the financial world conducts its business operations with speed, certainty and confidence" [40].

I plan to perform semi-structured interviews. Indeed, as seen, the AML sprocess involves many entities with many actors in many countries. People implicated in this process can have very different profiles and during their carreer they can have meet more than one of the three systems composing the AML information system (technical, formal and informal). Moreover, these systems are independant but interrelated. Therefore, a person linked to the AML process can bring information as well at the technical, formal or informal level because during his carreer this person has been confronted to these three interrelated systems.

I plan to keep in mind the structure in three levels (technical, formal and informal) and the limits for the ML detection efficiency about each of these levels

highlighted in this thesis like analytical grid for future interviews.

The figure 6.1 illustrates an example of the grid that I plan to use.

level	problem	subproblem
technical		
	A lack of learning	
	A specific database format	
	Configuration difficulties	
	Too many detection errors	
formal		
	Lack of strictness in the interpretation of international directives in national laws	
		AML not a national priority
	Lack of strictness in the translation of national laws into local methods and procedure	
informal		
	Negative attitude towards AML	
	No motivation	
	A lack of training	
	A lack of capabilities	
	A lack of awareness	

Figure 6.1: Example of analitical grid

For example, if I meet someone more oriented at the technical level, firstly, I plan to recolt information which can confirm or refute the first limits of the AML technical systems highlighted in this thesis. Next, I plan to discuss about other limits they have met during their carreer at the technical level and the possible solutions that can solve these limits from their expertise keeping in mind solutions proposed in this thesis. But I also want to let them discuss about subjects around the technical system which can enrish my analysis at the formal and/or informal level.

I plan to perfom in the same way for people more oriented in the formal or in

the informal level: keeping in mind the structure in three levels and the first results about each level. More interviews I have more my analytical grid can be enrished and more each interview can have reference points for the discussion.

I'm persuaded that my formation in information management between the business and the computer science could bring me a advantage to collaborate with people from the technical system and people from the formal and informal one.

Bibliography

[1] Loi du 11 janvier 1993 - loi relative la prevention de l'utilisation du systme financier aux fins du blanchiment de capitaux et du financement du terrorisme.

[2] Oxford concise english dictionary, tenth ed. *Publisher.*

[3] Internation federation of accountants - web.ifac.org/.../2/...money.../anti-money-laundering-2n.pdf, 2004.

[4] Bonnie Buchanan. Money laundering-a global obstacle. *Research in International Business and Finance 18.*

[5] Ana Isabel Canhoto and James Backhouse. Profiling under conditions of ambiguity-an application in the financial service industry. *Journal of Retailing and Consumer Services 14.*

[6] Celent. Evaluating the vendors of anti-money laundering solutions - http://reports.celent.com/pressreleases/20060829/aml vendors 2006.htm, 2006.

[7] Remco Chang, Mohammad Ghoniem, Robert Kosara, William Ribarsky, and Jing Yang. Wirevis:visualiation of categorical, time-variant data from financial transactions. *IEEE Symposium on Visual Analytics Science and Technology 2007.*

[8] Tat-Man Cheong and Yain-Whar Si. Event-based approach to money laundering data analysis and visualization. 2010.

[9] C.Phua, V.Lee, K.Smith, and R.Gayler. A comprehensive survey on data mining-based fraud detection research. *Artificial Intelligence Review.*

[10] Simon Davies. A year after 9/11: Where are we now? *Communications of the ACM.*

[11] FATF. The fatf recommendations. 2012.

[12] Tutorial fof Weka https://blog.itu.dk/SPVC E2010/file/2010/11/wekatutorial.pdf.

[13] Shijia Gao and Dongming Xu. Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering. *Expert systems with applications*, 36:1493–1504, 2009.

[14] Shijia Gao and Dongming Xu. Real-time exception management decision model (rtemdm): applications in agent-assisted decision support in logistics and anti-money laundering domains. *Proceedings of the 43rd hawaii international conference on system sciences*, 2010.

[15] Shijia Gao, Dongming Xu, Huaiqing Wang, and Peter Green. Knowledge-based anti-money laundering: A software agent bank application. *Journal of knowledge management*, (2):63–75, 2009.

[16] J. Han and M. Kamber. Data mining: Concept and techniques. *Morgan Kaufmann publishers, 2nd Eds.*

[17] Agents intelligents http://www.agentintelligent.com/agent intelligent/agents intelligents.html.

[18] J.Thang and J.Yin. Developing an intelligent data discreminating system of anti-money laundering based on svm. *Proceedings of the Four International Conference on Machine Learning and Cybernetics.*

[19] J.Wang, Y. Liao, T.Tsai, and G.Hung. Technology-based financial frauds in taiwan: issue and approaches. *IEEE conference on: System, Man and Cyberspace.*

[20] Nhien An Le Khac and M-Tahar Kechadi. Application of data mining for anti-money laundering detection : A case study. *IEEE international conference on data mining workshops*, 2010.

[21] Nhien An Le Khac, Sammer Markos, and M-Tahar Kechadi. A data mining-based solution for detecting suspicious money laundering cases in an investment bank. *Second international conference on advances in databases, knowledge, and data applications*, 2010.

[22] Xuan Liu and Pengzhu Zhang. Research on constraints in anti-money laundering (aml) business process in china based on theory of constraints. *Proceedings of the 41st Hawaii International Conference on System Science.*

[23] Xuan liu and Pengzhu Zhang. A scan statistics based suspicious transactions detection model for anti-money laundering(aml) in financial institutions. *International Conference on Multimedia Communications.*

[24] Xuan liu, Pengzhu Zhang, and Dajun Zeng. Sequence matching for suspicious activity detection in anti-money laundering. *ISI Workshops.*

[25] E.W.T. Ngai, Yong Hu, Y.H. Wong, Yijun Chen, and Xin Sun. The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature. 2010.

[26] Interview of Madam Anne Goldfischer; Compliance Officer at the Bank Degroof, 04/05/2012.

[27] Interview of Mister Christian Tournie; D.G Internal affairs detached national Expert to the European Commission, 2011.

[28] Interview of Mister Markus. E. Schulz; Chief Compliance Officer Life and Group Compliance at Zurich Life Insurance Compant Ltd Group Financial Crime Officer, 2012.

[29] The European Parliament and the Council of the Europe. Directive 2005/60/ec of the european parliament and the council of 26 october 2005 on the prevention

of the use of the financial system for the purpose of money laundering and terrorist financing. *Official Journal of the European Union.*

[30] Norton T. Roman, Christiano D. Ferreira, Luis A.A. Meira, Rodrigo Rezende, Luciano A. Digiampeitri, and Jorga Jambeiro Filho. Attributvalue specification in customs fraud detection; a human-aided approach. *The Proceedings of the 10th International Digital Governement Research Conference.*

[31] Jean Spreutels. Le groupe d'action financiere (gafi) et la lutte contre le blanchiment de capitaux - www.ctif-cfi.be/doc/fr/articles/s1v10041.pdf, 1996.

[32] Yingfeng Wang, Huaiqing Wang, Shijia Gao, Dongming Xu, and Kang Ye. Agent-oriented ontology for monitoring and detecting money laundering process.

[33] Official website of aci. The aci automated case management system for anti-money laundering - http://search.tsainc.com/pdfs/aci and http://www.aciworldwide.com.

[34] Official website of CBFA http://www.cbfa.be/fr/index.asp.

[35] Official website of CTIF-CFI http://www.ctif cfi.be/.

[36] Official website of fiserv http://www.financialcrimerisk.fiserv.com/anti money-launderingmonitoring.aspx.

[37] Official website of gafi http://www.fatf gafi.org.

[38] Official website of i-ight http://www.customerexpressions.com.

[39] Official website of Nokom. Norkom's anti-money laundering (aml) solution - http://www.norkom.com/solutions/anti-money-laundering.html.

[40] Official website of SWIFT http://www.swift.com/about swift/index.page?

[41] Official website of the Egmont Group http://www.egmontgroup.org/.

[42] Official website of the United Nations Office on Drugs and Crime http://www.unodc.org/unodc/en/treaties/CTOC/.

[43] Wikipedia. Anti-money laundering software - http://en.wikipedia.org/wiki/anti-money laundering software.

[44] Z. Zang, J.J. Salermo, and P.S Yu. Applying data mining in investigation money laundering crimes. *SIGKDD'03.*

[45] Gao Zengan. Application of cluster-based local outlier factor algorithm in anti-money laundering. 2009.