ADDIS ABABA UNIVERSITY
SCHOOL OF GRADUATE STUDIES
DEPARTMENT OF COMPUTER SCIENCE

Anti Money Laundering Software Framework for Ethiopian Banks and Financial Agents

Yalemie Temesgen Demeke

A THESIS SUBMITTED TO

THE SCHOOL OF GRADUATE STUDIES OF ADDIS ABABA UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF MASTER OF SCIENCE

IN COMPUTER SCIENCE

June 2014

ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

DEPARTMENT OF COMPUTER SCIENCE

Anti Money Laundering Software Framework for Ethiopian Banks and Financial Agents

Yalemie Temesgen Demeke

Advisor: Dejene Ejigu (PhD)

Approved By:

Examining Board:

1. Dr. Dejene Ejigu, Advisor _____

2. _____ _____

3. _____ _____

Acknowledgment

My first and deepest thanks goes to the Almighty God. Had not been God with me, my dreams in Computer Science would not have been real.

Next, I would like to express my deepest gratitude to my advisor Dr. Dejene Ejigu for his encouragement and my research idea become touchable. Also I would like to thank all professors and instructors of the department of computer science, Addis Ababa University.

Finally, I would like to thank my family for their continuous support, moral and initiative throughout the thesis work, especially my brother Alemayehu Temesgen and my wife Yetnayet Asmer.

Table of Contents

List of Tables

List of Figures

List of Algorithms

Acronyms

ADO.NET :	ActiveX Data Object.NET
AML :	Anti Money Laundering
APG:	Asia/Pacific Group on Money Laundering
BLL :	Business Logic Layer
CAR:	Cash Activity Report
CDD:	Customers Due Diligence
CD-R:	Compact Disc-Recordable
CFATF:	Caribbean Financial Action Task Force
CFT :	Combating the Financing of Terrorism
CPO :	Customer Payment Order (banking)
CTR:	Cash Transaction Reporting
CRUD :	Stands for create, read, update, and delete
DAL :	Data Access Layer
EAG:	Eurasian Group
EFIC:	Ethiopia Financial Intelligence Center
ESAAMLG:	Eastern and Southern Africa Anti Money Laundering Group
FATF:	Financial Action Task Force
FI :	Financial Institution
FIC:	Financial Intelligence Center
FIU	Financial Intelligence Unit
FRC :	Financial Reporting Center
FSRBs:	FATF-Style Regional Bodies
FT:	Financing of Terrorism
GAFISUD:	Financial Action Task Force on Money Laundering in South America
GIABA:	Inter Governmental Action Group against Money Laundering in West Africa
IMF:	International Monetary Fund
KYC:	Know Your Customer
LINQ :	Language Integrated Query
MA	Master of Art
MENAFATF:	Middle East and North Africa Financial Action Task Force

ML:	Money Laundering
MONEYVAL:	Council of Europe Committee of Experts on the Evaluation of Anti Money Laundering, Measures and the Financing of Terrorism
NPS:	National Payment System
OWL	Web Ontology Language
PEP:	Politically Exposed Person
POCAMLA:	Proceeds of Crime and Anti Money Laundering
POS :	Payment Ordered System
SPARQL	Standardized Protocol and RDF Query Language
SQL :	Structured Query Language
STR:	Suspicious Transaction Report
SW	Software
SWRL	Semantic Web Rules Language
UI :	User Interface
XML:	Extensible Markup Language

Abstract

Money Laundering (ML) is the crime of transforming illegally obtained income into seemingly legitimate funds in banks. Anti Money Laundering (AML) is a set of rules or regulations enacted to stop the practice of generating income through Money Laundering and to stop the international and local money launderers. Money Laundering is a major problem in many countries of the world which arises from the difficulty to prevent, detect and prosecute illegal income generation and money transfer. Recent information technologies are making money laundering easier to deposit or withdraw and transfer their funds using financial systems. Hence, controlling ML requires implementation of sophisticated mechanisms.

This research sought devising computer based AML mechanism for Ethiopian Banks and Financial Agents by designing a software framework for cash and suspicious data handling, processing, detection avoidance report and remittance monitoring and cash data validation. The Ethiopia Financial Intelligence Center (EFIC) was established by the Ethiopian Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation to develop appropriate information management systems to ensure the protection of sensitive and confidential financial information disclosed to supervisory authority. However, there was no computer based AML solutions. Accordingly, this research sought to develop framework with which banks and agents could better control and prevent ML.

The result of the framework also supports cash data validation and remittance monitoring for National Bank of Ethiopia (NBE). The framework is tested and validated by using selected data collected from banks and financial agents and by prototype mainly using individual National ID. The prototype developed for that purpose allows the handling of bulky data from various sources and detects suspicious transactions. The framework suggests how to handles, process and report risky financial transactions according to the relevant policy and strategy of the country in ways that help the works of EFIC easier and more effective.

Keywords: Money Laundering, Anti Money Laundering, Ethiopian Banks and Financial Agents, National Bank of Ethiopia, Ethiopia Financial Intelligence Center.

Chapter One: Introduction

1.1 Background

Money Laundering (ML) is the crime of moving money that has been obtained illegally through banks and other businesses to make it seem as if the money has been obtained legally. Money laundering is illegal. Anti Money Laundering (AML) is a set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions [10].

Today, money laundering is becoming more and more sophisticated. This criminal activity poses a serious threat not only to financial institutions but also to nations [1]. Most international financial institutions like banks and financial agents have been implementing Anti Money Laundering solutions. However, most of the existing commercial solutions are not effective enough for countries like Ethiopia. Those solutions need a lot of customization to directly implement Anti Money Laundering rules, regulations and procedures, and therefore are not full-fledged solutions, especially for detecting and analyzing suspicious transaction.

There are three stages to Money Laundering: these are Placement, Layering, and Integration [2].

- The first time funds derived from criminal activities are used in a legitimate money transfer is referred to as **Placement**.
- Creating a series of transactions to hide the first transaction is referred to as **Layering**.
- The return of funds to legitimate activities is referred to as **Integration**.

In the case of Money Laundering the funds destined would be integrated into the national economy through banks.

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter these problems [3].

According to the Ethiopian Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation [4], the Ethiopian Financial Intelligence Center (FIC) was established to collect, analyze and disseminate information to law enforcement bodies. Therefore Ethiopian Banks and Financial Agents provide Cash Transaction Report (CTR) and Suspicious Transaction Report (STR) to Ethiopia Financial Intelligence Center (EFIC). Based on the rules and regulations, Ethiopian Banks and Financial Agents are obliged to report all cash deposits or withdrawals and remittances exceeding or equal to Birr 200,000.00 or 10,000.00 USD or its

equivalent in other foreign currency. At the same time they classified the transaction into two: cash transactions and suspicious transactions. In this research, financial institutions are institutions that process any kind of banking or non-banking transactions through cash, cheques, Customer Payment Order (CPO) and so on, including foreign and local remittances. Therefore, financial institutions in this research refer to Ethiopian Banks and Financial Agents.

As pointed out above, ML is a threat for countries and nations, and also it is highly risky to financial institutions as it could damage the national economy of a country. Hence, the governments, financial regulatory bodies and financial institutions require implementing processes and procedures to prevent or detect money laundering from their illegal activities that money launderers are involved in. To do this jurisdictions have understood the critical significance of national financial stability and international security by using Anti Money Laundering mechanisms.

Financial institutions have been working manually for collecting, analyzing and dissemination of transactional data in collaboration with EFIC experts. Using traditional manual work to identify suspicious transactions from all collected huge data from financial institutions and agents is very difficult and labor-intensive task.

The challenges of implementing AML in financial institutions are large due to the growing volume of transactional data, nature of money laundering and heterogeneity and diversified place of data. In order to tackle such challenges solution developers have tried a lot but have not succeeded in generating software architecture and developing solutions. Indeed, the volume of financial institutions and transactions has increased manifold and managing ML under such circumstances needs to be supported by automated tools.

In order to develop effective software that is highly integrated to the financial systems, it is necessary to create the software framework that supports and fully address the AML objectives. The AML software framework can address the problem of ML from its starting point of money placement. At this stage the financial institutions should have their own KYC policy and identify their own customers. The automated intelligent tools can support the users to follow up suspicious transactions from the start.

A number of banks and financial agents placed in different areas have data about the customers' transactions and needs to be reported to EFIC. There need to be a data collection mechanism for use by EFIC so that quick analysis and response would be possible. Once data is supplied to EFIC from different sources, it is necessary to change the collected data into one of the required file format to make subsequent analysis of suspicious transactions smoother. Given the bulky

nature of data and growing complexity of transactions due to the employment of state-of-the-art technology, it is obsolete to hang on using the manual technique of data collection and analysis. It is thus high time that the country's financial system combat money laundering through the application of automated tools.

After the EFIC operation is completed, the next process is reporting of the results to the concerned government authorities for the appropriate response. Finally, without the help of automated tools, it is very difficult to attain the goal of AML. Conversely, with the help of efficient automated tools it would not be a wild dream to realize a decrease to the problem of the increasingly sophisticated techniques of money launderer's.

1.2 Statement of the Problem

FATF report on June 22, 2012 stated that Angola, the People's Democratic Republic of Korea, Bolivia, Ecuador and Ethiopia have been named as jurisdictions that have not committed to the FATFs action plan and the international Anti Money Laundering standards [3]. After the establishment of EFIC the center collects CD which contains transaction records in Access database file format from banks and agents to analyze and disseminate the report. The data collection process is supported by EFIC standalone system.

Even though EFIC has deployed standalone system for fully operational and effectively functioning Financial Intelligence Center, but still to this date, Ethiopia does not improve the commitment on Money Laundering. Among them, Ethiopia is a highly risky country and non-cooperative in action of Anti Money Laundering by FATF [5, 6].

Though the government is willing and put in place a center for the purpose, the major problem is data collection, analyzing, investigating and reporting of cash and suspicious transactions from different Ethiopian Banks and Financial Agents, and reporting to FATF accordingly.

1.3 Objectives

General Objective

The general objective of the thesis is to design the AML Software framework, needed to handle and process Cash and Suspicious Transactions of Ethiopian Banks and Financial Agents.

Specific Objectives

The specific objectives of the study include:

- Understand ML and its controlling mechanisms worldwide.

- Identify the relationship between Information Technology and AML data handling mechanisms.
- In-depth study of challenges encountered while implementing AML in Ethiopia.
- Study FATF rules and procedures for Cash and Suspicious Transaction in Ethiopian Banks and Financial Agents.
- Study nature of transaction data format generated from different Ethiopian Banks and Financial Agents.
- Create a single data format for cash and suspicious transactions collected from different Ethiopian Banks and Financial Agents.
- Study the possibility of setting unique customer ID for Ethiopian Banks and Financial Agents identification mechanism.
- Propose the report format of financial transaction details to FATF as per the requirements.
- Design AML software framework for Ethiopian Banks and Financial Agents.
- Create a prototype of the proposed AML Software framework.
- Test and validate the framework.

1.4 Methodology

A concise elucidation of the methodology will be elaborated under this section. The following lists of methodology are used to realize AML Software framework for Ethiopian Banks and Financial Agents:

- **Literature Review and Related Works**

In this research, a number of published research papers; complete thesis works; books and web sites in the area of Anti Money Laundering in general and software framework design process in particular are observed.

  - Review the methods of different countries experience on AML
  - Study related works on AML techniques and ML controlling mechanisms.

- **Data Collection**

In order to come up with one data format and to create a prototype for the AML software framework it is necessary to collect sample data from different sources, i.e., Ethiopian Banks and Financial Agents.

- **Prototyping**

To validate the proposed framework design and algorithms recommended in this work, we use a prototype as a means of proving the concepts.

1.5 Application of Results

The FIC work shows that-despite the high motivation of government and international bank framework to reduce money laundering attacks, the center faces many problems regarding the cash and suspicious transactions data. This research designs a software framework and shows the prototype of handling and processing of data on cash and suspicious transactions collected from Ethiopian Banks and Financial Agents.

These are some of the benefits of this research:

1. Support to develop fully integrated AML solutions for Ethiopian Banks and Financial Agents.
2. Helps to implement FATF rules and procedures based on Ethiopian context which is used for handling and processing of Financial Transactions (data entry, analysis, investigation and reporting).
3. Shows how to improve delivery time of the service for data collection, analysis, investigation and reporting for FIC.
4. Helps researchers on AML in Ethiopian Financial Institutions in identifying the area of the problem, in minimizing the ML problems and in finding the solutions for ML problem.
5. The framework recommends identifying transactions (i.e., Cash and Suspicious) using standardized unique ID for customers of financial institutions.

1.6 Scope and Limitations

The scope of this research is limited to Ethiopian Banks and Financial Agents. The research does not include insurances and micro finance institutions. The AML Software framework for Ethiopian Banks and Financial Agents includes only the following components:

- Know Your Customer (KYC) Schema for clients and customers of the Ethiopian Banks.
- Cash and Suspicious Data Handling for the Banks and Financial Agents.
- Cash and Suspicious Activity Process models for Ethiopian Financial Intelligence Center.
- Remittance Monitoring and Cash Data Validation for National Bank of Ethiopia.

Most of the activities of the framework depend on individual National ID. During the start of this research we asked the office, Federal Democratic Republic of Ethiopia Security Immigration and Refugee Affairs Authority, and as per the authority information they will implement the project in the near future. The framework does not implement for law enforcement bodies rather it will generate detection avoidance report to the system of law enforcement parties.

Limitation of the framework at this time is getting the National ID of an individual who is involved in banks and financial agent's transactions. With what criteria this National ID is created to identify an individual.

1.7 Organization of the Thesis

This thesis document has six chapters excluding the current chapter. Literature Review is discussed in Chapter 2. The concept of Money Laundering, FATF and FIC, Information Technology and AML, FATF Recommendations for Ethiopia and AML in Ethiopia, KYC and Customer Due Diligence (CDD), Ethiopian Prevention and suppression of Money Laundering and Financing of Terrorism Proclamation are its major sections. Chapter 3 deals with common features of others' works related to this thesis. Chapter 4 discusses the details of the proposed design, provides components of the proposed framework and their algorithm. Description of the framework and its prototype with general description of implemented components and demonstration is given in Chapter 5. Chapter 6 deals with Evaluation and Testing. Chapter 7 provides conclusion of the study and future work.

Chapter Two: Literature Review

2.1 The Concept of Money Laundering

2.1.1 The Origin and Meaning of Money Laundering

Money laundering is a significant problem in many countries of the world which arises from the difficulty to prevent, detect and prosecute illegal income generation and money transfer. Given the harm it causes to the economy of a given country through the proliferation of dirty money, it has been criminalized by many governments. According to Bill's Money Laundering Information Website the term "money laundering" is said to have originated from Mafia ownership of *Laundromats*[1] in the United States in which gangsters were implicated in earning huge sums of money in cash from extortion, prostitution, gambling and bootleg liquor" [7]. Similarly, Singh traces the history of money laundering to that Mafia group [8]. On their part, Laundromats and Laundromats followers contended that they derived their money from legitimate rather than criminal activities.

There is no single definition for Money Laundering agreeable to different writers. However, all definitions concur on the view that Money Laundering is a sophisticated crime of moving illegally obtained money through banks using techniques that give the movement a semblance of legal backing. Most of the researchers and AML scholars agree that Money Laundering is not an independent crime as it depends upon another crime and the proceeds thereof become illegal. In fact hiding of the source of the fund by itself might not be a crime but proceeds from criminal activities will be illegal.

Money Laundering is the form of transnational and organized crime which is prevented or limited by designed anti money laundering exertions. Money Laundering generally involves a series of multiple transactions used to disguise the source of financial assets so that those assets may be used without compromising the criminals who are seeking to use them [9]. Regardless of the crime involved, money launderers move their illegal funds using three ways: placement, layering, and integration [10]. The Money Laundering Cycle [11] by United Nations Office on Drugs and Crime as shown in Figure 2.1.

[1]A service mark used for a commercial establishment equipped with washing machines and dryers, usually coin-operated and self-service. This is excerpted from The American Heritage Dictionary of the English Language, Third Edition.

Figure 2.1 : Money Laundering Cycle

1. Placement

The first stage of the Money Laundering process involves placement of illegally derived funds into the financial system, usually through banks and financial agents using financial instruments[2] for converting their illegal funds.

2. Layering

The second stage of Money Laundering is when the ill-gotten funds placed in banks are transferred into other sources using any form of negotiable instrument such as cheques, money order or bearer bond, or they may be transferred electronically to other accounts in various jurisdictions.

3. Integration

The third stage involves the integration of funds into the legitimate national economy. This is accomplished through the purchase of assets, such as real estate, securities or other financial assets, or luxury goods.

2.1.2 Who are Money Launderers?

Money Laundering is being employed by Money Launderers worldwide to conceal their criminal activities. Those Launderers predominantly employ legal cash transactions to hide the true ownership and source of the money. Under the guise of legal cash transactions and transfers, Money Launderers manage to conceal the source, nature, place, deposition and movement of

[2] Financial Instruments are tools used in Financial Institutions to make transactions. CPO, Cheques and Hawallas are some of the examples of Financial Instruments. Financial Instruments have the same meaning to negotiable instrument in this document.

their illicit proceeds in ways that would make their money as if earned through legitimate means. In order to fight against them it is necessary to access certain financial information and to conduct financial investigations. The principal goal of financial investigation is to identify, trace and locate illegal fund and subject it to legal measures by taking responsible persons to justice.

As per evaluation of FATF [21] illicit financial operations, carried out through Ethiopian Banks and Financial Agents, are becoming more sophisticated and complex to the extent that it has become difficult to distinguish legal from illegal financial dealings. This is mainly due to the inefficiency of the traditional financial investigation mechanisms that make attempts of investigating complex operations very difficult and hectic. From that difficulty was born the need for countries to design and implement advanced techniques of financial investigation with the help of modern and specialized financial intelligence tools. Financial intelligence tools are used to support a comprehensive track down of Money Launderers by analyzing relevant data reported to financial investigations.

2.1.3 Damage of Money Laundering

The negative effects of money laundering on economic development are difficult to quantify. It is clear that such activity damages the financial systems of the countries [12.

Money laundering has been a global problem since the beginning of the 20thcentury and judicial measures have been adopted against it. This criminal activity poses a serious threat not only to financial institutions but also to nations [1]. The official site of FATF estimated that the damage of ML on the world's economy in 2009 is equivalent to 3.6% of global GDP, which means that about 1.6 trillion USD is being laundered every year [13].

2.1.4 What is Anti Money Laundering?

In contrast, Anti Money Laundering refers to a set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions or Money Laundering. Most of the Ethiopian Banks and Financial Agents locally and internationally have been implementing Anti Money Laundering solutions to fight against criminal activities. Implementing Anti Money Laundering in jurisdictions is highly significant to national financial systems and international security. Traditional approaches to the AML followed a labor intensive manual approach for data collecting, analysis and dissemination of financial disclosures.

2.2 Financial Action Task Force and Financial Intelligence Center

2.2.1 Financial Action Task Force

To combat Money Launderers, countries decided to establish, organize and coordinate a Financial Action Task Force (FATF) in 1989 under the leadership of the Finance Ministers of member states. The main objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering. Thus, FATF is an intergovernmental policy making body, comprised of over 30 countries empowered to set AML mechanisms for controlling the transfer of ill-gotten funds. Above 180 jurisdictions have joined the FATF or an FATF style regional body that are represented by their finance ministers, to implement the FATF standards for anti money laundering. FATF has given to all countries its methodology of assessing compliance with the FATF 40 Recommendations against Money Laundering.

Over 180 countries admit that Money laundering is a truly global phenomenon [8]. The increasing integration of the financial system locally and internationally with the help of technology has eliminated barriers for the movement of capital in ways that assist money launderers to easily clear traces of their ill-gotten gains. The technology has given money launderers ample leverage to quickly move the proceeds of their criminally derived property across national jurisdictions, thereby complicating the task of tracing and confiscating these assets.

2.2.2 Financial Intelligence Center

In his book entitled "Anti Money Laundry and Combating of Financial Terrorism", Schott [14] states that the Financial Action Task Force (FATF) on Money Laundering provides in the Forty Recommendations on Money Laundering to which each country should comply by establishing Financial Intelligence Unit. Besides to FATF recommendations countries understand the damage of Money Laundering and they establish their own Financial Intelligence Center (FIC) and work together all over the world in collaboration with FATF. AML solutions can be used in countries for FIC which works in coordination with local and international financial institutions.

According to Egmont Group's[3] definition "FIU is a central, national agency responsible for receiving (and as permitted, requesting), analyzing and disseminating financial information to

[3]The Egmont Group is an informal organization of financial intelligence units named after the location of the group's first meeting at the Egmont-Arenberg Palace in Brussels. The goal of the group is to provide a forum for FIUs to improve support to their respective national anti money laundering programs.

competent authorities" [15]. This definition is consistent to FATF recommendations regarding the role of FIC. The established FIC, according to "The Forty Recommendations of FATF" [16], has three essential core functions- receiving, analyzing and disseminating information to combat money laundering. Even if the organization and mandate of FIUs could vary from country to country, all of them share these three core functions. Both Financial Intelligence Unit (FIU) and Financial Intelligence Center (FIC) are the same and have the same goal. The dissemination of financial information of the country should conduct at domestic and international levels. Because Money Laundering is a cross-border issue [17] it is necessary that each FIU should have international financial information sharing mechanisms with its counterpart in other countries. That is an essential prerequisite to effectively halt money laundering. Each FIU should be empowered to use a centralized repository for the reporting of financial information. This requires that all of the relevant information need to be deposited in one central place. The task of analyzing financial information must be carried out in a consistent manner for each country. Centralization also ensures greater efficiency in information gathering [14].

Financial transactions like custom deposits, withdrawals, fund transfers, or the purchase of a security contain pieces of information for detecting and accusing money laundering. In order to identify truly suspicious transaction it is not sufficient to use the most sophisticated data gathering tools unless the data obtained is analyzed properly. In particular, the FIU's analytical functions require extended powers to access information [14]. The powers include access to certain commercial or government databases; the authority to request additional information from reporting entities and other sources as necessary; and access to advanced intelligence techniques and apparatus, such as wiretapping and covert operations, subject to domestic legal principles.

Moreover, countries should decide according to the directives of FATF so that financial institutions handle their customers' or clients' identity details, in addition to their transactions data and, report any suspicious transactions which ever exists. Therefore, every financial institution in the country should have record keeping and reporting requirements[4] which generates extensive financial data to be reported to the country's FIC. The collected data might not be easily usable by competent authorities[5] before it is analyzed properly. To be all effective

[4]Record keeping and reporting requirements is the essential process to be done by banks and financial agents, which is used upon the request of competent authorities.

[5] Competent Authorities are government organs responsible for controlling ML in the country. Police Stations and Courts are Competent Authorities.

in data collecting, processing, analyzing and disseminating of the financial information to competent authorities, FIC should adequately be supported by automated tools.

2.3 Countries and their ML Controlling Mechanisms

As mentioned above, FATF has forwarded recommendations in what is known as the global Anti Money Laundering standard. To accomplish global standard implementation of the FATF Recommendations, the FATF trusts on a strong global network of FATF-Style Regional Bodies (FSRBs). The FSRBs have an essential role in promoting the effective implementation of the FATF Recommendations by their membership and in providing expertise and input in FATF policy-making. According to the official site of FATF [13] the members of FATF are: Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Eurasian Group (EAG), Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG), Financial Action Task Force on Money Laundering in South America (GAFISUD), Inter Governmental Action Group against Money Laundering in West Africa (GIABA), Middle East and North Africa Financial Action Task Force (MENAFATF) and Council of Europe Committee of Experts on the Evaluation of Anti Money Laundering, Measures and the Financing of Terrorism (MONEYVAL). From these, the networked FATF style, ESAAMLG, is benchmarked for this study since it contains countries like South Africa and Kenya whose experience could easily be adapted to the Ethiopian circumstances.

2.3.1 South Africa

South Africa is the member of FATF and which is the member of ESAAMLG. South Africa has implemented AML preventative measures through the application of the Financial Intelligence Center. The joint committee of Financial Action Task Force (FATF) and its regional body, the Eastern and Southern Africa Anti money laundering Group (ESAAMLG) approved that the government in South Africa has demonstrated a strong commitment to implement AML systems, which has involved close cooperation and coordination between a variety of government departments and agencies [24]. The Mutual Evaluation was to illustrate that the architecture of South Africa's AML framework is the essential building block of its anti money laundering.

The Financial Intelligence Center of South Africa is organized under the Ministry of Finance. The Center has a well-structured, funded, and staffed FIC that is functioning effectively. The Center became a member of the Egmont Group of Financial Intelligence Units in 2003 and has access to a wide range of financial, administrative and legal backing to enhance its ability to analyze Suspicious Transaction Reports. The center is also authorized to request additional

information from reporting entities and has issued guidance on the reporting obligation and provides feedback to its stakeholders.

Financial institutions covered by the FIC, so called accountable institutions, are prohibited from establishing a business relationship or concluding a single transaction with a customer before establishing and verifying the customer‘s identity, and the identity of any person acting on behalf of the customer or on whose behalf the customer is acting. Accountable institutions are also required to establish and verify the identity of all customers with whom it had entered into a business relationship before the FIC regulations took effect, so called existing customers. In South Africa FIC is supported by an intelligence tool which is used to collect, analyze and disclose financial information to competent authorities. Besides, the FIC has a web site where it organizes the data collection of cash and suspicious transactions [18].

Following the last FATF mutual evaluation of South Africa (2003), the Government established a project team to implement changes to South Africa's National Payment System (NPS) which would enable full registry of originator information for domestic and international transfers using the SWIFT[6] messaging formats. The system ultimately relies on the operating rules and standards that govern the National Payment System (NPS) and the contractual obligations among NPS participants to comply.

Both South Africa's NPS and FIC web site are useful for controlling Money Laundering in South Africa. The South Africa FIC web site allows users to register Suspicious Transactions and suspected terrorist actions.

The principal objective of South Africa's FIC office is combating money laundering. FIC is responsible to the overall "value chain" process to work effectively with legal authorities. This means that South Africa's anti money laundering work has a single system or a "value chain", which involves the coordinated and integrated efforts from a wide range of different partners. The partners range from the business sector like banks and agents, the supervisory bodies, FIC, the law enforcement authorities and the prosecution services. Besides Asset Forfeiture Unit works together with them to seize the assets involved in money laundering and the criminal activities. The role of every organ is depending on one to another. The country has developed the framework as shown in Figure 2.2 to work as one unit.

[6] SWIFT is global provider of secure financial messaging service to transfer money by banks and financial agents. SWIFT is Society for Worldwide Interbank Financial Telecommunication. Site www.swift.com.

The center receives customers and report of suspicious transactions from banks, insurances and casinos and analyzes the reports and to refer to investigative authorities and intelligence agencies. They are supported by the intelligent system as a whole. They are not fully functional or effective if the different component parts do not properly function as a unit within this chain.

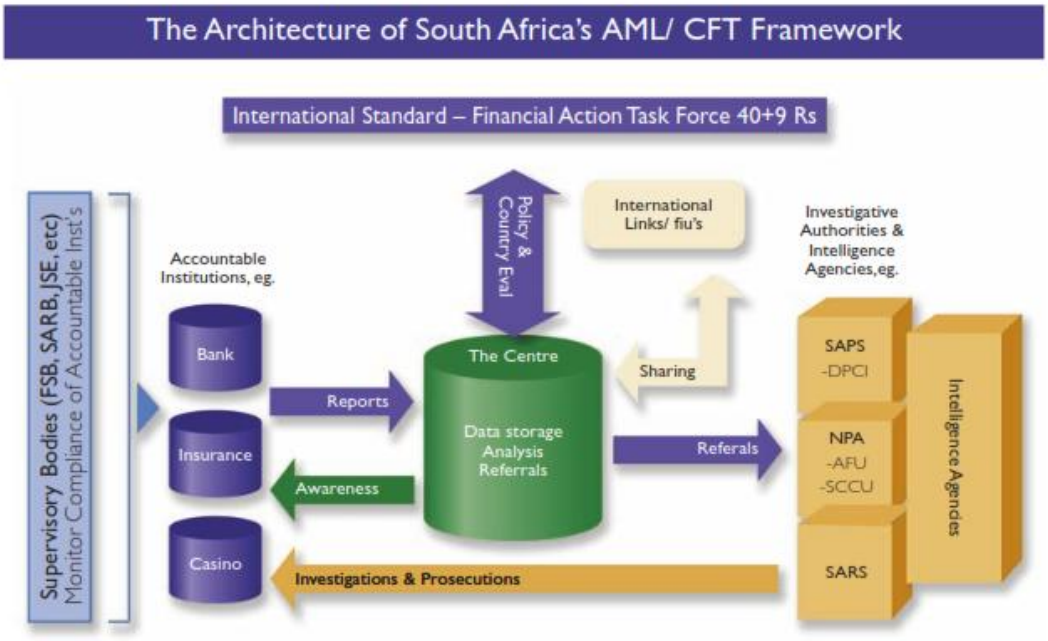


Figure 2.2 : The architecture of South Africa's AML/CFT Framework

2.3.2 Republic of Kenya

Republic of Kenya is the member of ESAAMLG and committed to be compliant but not to have progressed history in AML. As regards the AML system, the Republic of Kenya is still in an early stage of development and much work needs to be done with regard to the implementation of the AML measures, capacity building and awareness-raising within the reporting community and the general public.

The Proceeds of Crime and Anti Money Laundering Act in 2009, i.e., POCAMLA is the primary enactment which supports the AML legal framework in Kenya. Kenya does not have an operational FIC yet. The POCAMLA provides for establishment of the Financial Reporting Centre (FRC) as a national center to receive, analyze and disseminate financial intelligence and information. Presently, the Central Bank of Kenya receives suspicious transaction reports from banks and other financial institutions falling under its supervisory mandate. The regulatory framework in Kenya does not address the risk of money laundering. Under the provisions of the POCAMLA all financial institutions are required to take reasonable measures to establish and

verify the identity of all customers regardless of the level of risk associated with that customer or the transaction. Reporting institutions are required to monitor on an ongoing basis all complex, unusual, suspicious, large or other transaction as may be specified in regulations, whether completed or not.

Every FATF-Style Regional Bodies like ESAAMLG have evaluated their members, the evaluation of the anti money laundering regime of countries was based on the Forty Recommendations of the Financial Action Task Force (FATF), and which was prepared using the AML Methodology [15]. The evaluation was conducted by an assessment team, which consisted of members of the FATF Secretariat and FATF experts for examining the capacity, the implementation, and the effectiveness of all the systems including FIC systems.

2.4 Financial Action Task Force Recommendations for Ethiopia

The Financial Action Task Force on Money Laundering, which is recognized as the international standard setter for Anti Money Laundering, provides recommendations.

The FATF recommendations to control Money Laundering globally are called The Forty Recommendations on Money Laundering (or The Forty Recommendations). Assessing literature on the actual performance of the country is highly daunting for the research theme is uncommon for previous researchers. Nevertheless, Biniam Shiferaw [20] argued that the gap between the experience of Ethiopia and the outside world in the fight against money laundering is so huge. Biniam Shiferaw thus recommends that efforts should be exerted towards tackling ML mainly from the banking perspectives.

The official statement of the FATF on 12 of October 2012 [21] stated that

> *"Ethiopia has taken steps towards improving its AML/CFT regime, including by building up its Financial Intelligence Unit. However, despite Ethiopia's high-level political commitment to work with the FATF to address its strategic AML/CFT deficiencies, Ethiopia has not made sufficient progress in implementing its action plan, and certain strategic AML/CFT deficiencies remain. Ethiopia should continue to work on implementing its action plan to address these deficiencies, including by: (1) adequately criminalizing money laundering and terrorist financing; (2) establishing and implementing an adequate legal framework and procedures to identify and freeze terrorist assets; (3) ensuring a fully operational and effectively functioning Financial Intelligence Unit; and (4) implementing effective, proportionate and dissuasive sanctions in order to deal with natural or legal persons that do not comply with the national*

AML/CFT requirements. The FATF encourages Ethiopia to address its remaining deficiencies and continue the process of implementing its action plan."

The quote illustrates that Ethiopia has made a remarkable progress in AML actions but still needs to be improved. The improvement can be done with the help of automated tools in order to fill the gap between international recommendations and Ethiopia's FIC activities. Before proposing how to fill the gap with the support of information technology, it is necessary to understand where the gap is. The problem lies in the gap between the realities of a given country and the standards of the Forty Recommendations on Money Laundering. It is very difficult to achieve excellence by imposing standards developed based on the circumstances of industrial countries without meticulous adaption to the economic, political and cultural milieu of a country.

For FATF a member country of Eastern and Southern Africa, Anti Money Laundering Group has conducted its own evaluation of Anti Money Laundering by an assessment team, which consisted of members of the FATF Secretariat and FATF experts. But Ethiopia is neither the member of FATF nor ESAAMLG, to do this evaluation with FATF.

For the action plan to be implemented in Ethiopia using FATF recommendations, a sound financial reporting system is a crucial element. Reporting of financial information from Ethiopian Banks and Financial Agents to EFIC is very important for analysis and investigation. The report includes two types of transactions: Suspicious Transaction Report (STR) and Cash Transaction Reporting (CTR).

2.5 Know Your Customer and Customer Due Diligences

Know Your Customer (KYC) is the basic issue of all anti money laundering rules and regulations. Ethiopian Banks and Financial Agents for money transfer around the world are thoroughly controlled to apply various rules for opening and conduct of accounts through KYC to eradicate the different kinds of losses. KYC is conducting customer due diligence which is the key part of customer identification, internal control and risk management of banks. KYC is crucial for banks to know their customer in order to minimize the risk of being exploited by money launderers to the Ethiopian Banks and Financial Agents and the country.

According to the FATF recommendations, banks must implement identification procedures of their customers through using what is called Customers Due Diligence (CDD). Moreover, Ethiopian Banks and Financial Agents must keep records and install system which handles the CDD, train the staff and monitor how customers are operating their accounts. Customers due diligence procedures are critical elements in the effective management of Banks and Financial

Agents risks against to ML as provided under FATF recommendation number 5 [4]. CDD is not just overseeing account opening operations and record keeping but require banks to formulate a customer acceptance policy of the institutions that involves extensive due diligence. In addition, this is important to identify suspicious activities.

KYC policy is an integral and prerequisite part for the business and activities of Banks and Financial Agents. Therefore, KYC is most closely associated with the fight against money laundering. The anti money laundering proclamation of Ethiopia recognizes the role to be played by KYC standards in fighting money laundering. Accordingly, the NBE has issued a directive on Customer Due Diligence of Banks Directive [22], which is highly focused on KYC policy.

Ethiopian Banks cannot open the accounts for the beneficiary by fictitious names. Therefore, it is necessary to check and clearly identify the identity of the clients. In addition, these clients of the institutions are classified into two categories: Natural and Legal persons and Politically Exposed Persons (PEP)[7]. The minimum KYC requirements for registering an individual or client should have:

- legal name including father and grandfather[8] name and all other names used;
- full permanent address of the account owner;
- telephone number, fax number and e-mail address, if available;
- date and place of birth, if possible;
- nationality;
- occupation, public position held and/or name of employer;
- type of account the client wants to open
- signed statement certifying accuracy of the information provided.

The type of account opened by the customer is provided as a requirement for identifying customers or clients. The other important category of clients is related to individuals who are otherwise known as PEPs. Financial transaction and business relationship with these individuals has higher money laundering risks and hence requires greater security than Natural and Legal people's financial transaction and accounts.

[7] According to the definition of NBE CDD "politically exposed persons" are individuals in a foreign country who are or have been entrusted with senior government functions, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;

[8] Grandfather name is applied in Ethiopia which is equivalent to father last name.

Then, the proposed solution framework should consider the KYC policy of Ethiopian Banks. And also financial agents and SWIFT handle money transfer from abroad to Ethiopia in foreign currency.

KYC policy is very essential for protecting a country's assets from money launderers. But the main challenge to the implementation of AML software framework, i.e., legal framework in the country is poor awareness creation and training initiative. The other hindrance to vibrant anti money laundering is devising automated instruments necessary to collect, receive, store, survey, analyze and disseminate financial information. Money transfer from abroad is essential for identifying the customer. Hence, the software framework design to provide IT solution to money laundering should consider this as one of the input for analysis of transaction data.

2.6 Ethiopian Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation

According to the Ethiopian Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation [4] the EFIC was established to run its activities receiving regulations issued by the Council of Ministers. The first responsibility of EFIC office is to collect, receive, store, survey, analyze and disseminate information to competent authorities. Besides, it is responsible to establish appropriate information management systems to ensure the protection of sensitive and confidential financial information disclosed to the supervisory authority. The following is the proclamation Article 3.13 (number 1 and 5) which is related to information technology and role of EFIC:

> "13. Powers and Duties of the Center-The Center shall without prejudice to its powers and duties specified under other provisions of this Proclamation:
>
> 1. collect, receive, store, survey, analyze and disseminate information concerning suspected money laundering and financing of terrorism in accordance with this Proclamation;
> 5. establish appropriate information management systems to ensure the protection of sensitive and confidential information disclosed to it under this Proclamation;"

To implement systematic information management systems, it is necessary to create the AML software framework which is fully conversant with different forms used by all Ethiopian Banks and Financial Agents to handle and identify money laundering.

2.7 AML in Ethiopia

Ethiopia is a country neither a member of any of FATF-Style Regional Bodies including ESAAMLG nor registered as members of FATF. FATF report on June 22, 2012 stated that Angola, the People's Democratic Republic of Korea, Bolivia, Ecuador and Ethiopia have been named as jurisdictions that have not committed to the FATFs action plan and the international Anti Money Laundering standards [3]. According to the recommendations of FATF Ethiopia has established EFIC in 2009, in order to collect, analyze and disseminate financial information from different financial institutions and agents in the country.

After the establishment of the EFIC which is responsible to collect CD's which contains Access database files from banks and agents for analysis and dissemination of the report. The data collection process is supported by EFIC standalone system. Even if EFIC has deployed standalone system for a full operational and effective functioning of the Financial Intelligence Unit, currently Ethiopia has not improved its commitment. That makes Ethiopia a highly risky country and non-cooperative to action of AML by FATF [3, 6].

There are immeasurable problems occurring in Ethiopia in implementing AML framework and working on FATF recommendations. Binaiam Shiferaw [20] listed the challenges of AML in Ethiopian Cash based payment system, unstable neighboring and porous borders, parallel banking activities (Hawallas) and inadequate capacity of law enforcement organs. Exactly these are the existing problems for implementing adequate AML framework but in order to attain successful implementation without IT automated software really it is very difficult.

A study by Biniam Shiferaw [20] essentially is about comparing the legal framework of the Ethiopian money laundering control and prevention with the corresponding internationally adopted principles and recommendations. Besides, it dealt with the role of advanced technologies to combat the problem of money laundering. The purpose of this research is to critically examine the anti money laundering framework of the country, the mechanisms to fight it and to suggest ways of enhancing the effectiveness of the law in achieving its objective in the banking sector.

The researcher strongly focused on the current expansion of new banks as financial institutions in Ethiopia, and the need of the issue of control and supervision of Ethiopian Banks and Financial Agents are special interest of the government to control money laundering. After detail research, the local law of the country for PEPs is excluded from special CDD requirements and financial institutions treat them like any other ordinary customer.

Biniam Shiferaw observed that the anti money laundering law of the country has provisions to fight money laundering in the banking sector but are not sufficient to fight it and its dire consequences.

The top two predicaments of the existing legal provisions that need to be amended are:

- Banks are required to report cash transactions in relation to deposits or withdrawals with a minimum threshold that is Birr 200,000.00 or 10,000 USD or equivalent of this amount in other currencies.

  Money Transfer from abroad is not included to report into Financial Intelligence Center which is the most important tool in the laundering process. Further, the provision about suspicious transaction reporting has also used ambiguous and uncertain words to be implemented.
- Banks should go further about KYC standards when searching for reliable and independent sources beyond ID card like payment bills, passport etc to avoid identity fraud.

  NBE should launch operation that makes sound use of guidelines set according to the principles of Know Your Customer, Suspicious Transaction Report and Cash Transaction Report requirements.

These two gaps identified by Biniam and necessary to address to solve the Ethiopian AML problems. In Ethiopia the number of Banks and Financial Agents has significantly increased over the last few years and is still increasing [31]. These banks and financial agents are involved to their potential customers' attraction by fast and reliable services. To win in the business competition, banks and financial agents provide effective and quality customer service using latest IT tools and mechanisms.

Money Launderers are attracted by payment systems like cash payments, using financial instruments, E-payment (Electronic Payment) systems, SWIFT, payment cards, Hawallas and others. Most of these payment systems are implemented in Ethiopian banks and financial agents which are used to hide their illicit activities of money launderers.

Information technology has been of great tool in running the operation of financial systems. New technologies are making money laundering easier to deposit their funds into financial system and also withdraw the funds by hiding their criminal activity they enter into the legitimate economy without suspicion. Most of the recent developments that technology makes possible have potential use for money laundering purposes. Similarly emerging use for money laundering risks

is identified in fund transfer through electronic mechanisms. Mobile Banking, Internet Banking and Payment Ordered Systems[9] are classified into this group.

Besides to the new technologies the heterogeneity of the systems used by Ethiopian banks and financial agents is the other concern. Most of the Ethiopian banks used their core banking solutions from which the financial information is generated and send to FIC [31]. The Financial information from different institutions and financial agents are quite different in their formats and descriptions, which needs to be the same format and descriptions for the same objectives.

Financial information is the most important element for EFIC, which is collected from different and many financial institutions and agents. The manual work of doing on financial information is traditional and very difficult. Therefore the main problem is collecting, analyzing and dissemination of financial information collected from financial institutions and agents have a great impact on implementing AML framework appropriately. This action is also highly important for implementing and enhancing the evaluation of FATF recommendations for the country.

A country's effectiveness in the fight against money laundering is dependent upon the strength and weakness of its financial investigation authorities. The financial investigation authorities are designated to EFIC which is highly dependent on financial information. EFIC, the pillar in the fight against money laundering should be organized effectively with the following objectives: collection and centralization of information, investigation and regulation function, national and international Information exchange and awareness creation [4].

The EFIC was set up with the purpose of investigating potential cases of money laundering activities and to ensure compliance of procedures by all accountable persons as well as enhancing public awareness and launching all necessary information management systems.

Suspicious Transaction Report is a fundamental element of international Anti Money Laundering system that requires financial institutions, including banks, to report their suspicion transaction to the concerned authority. Banks and financial agents are responsible of reporting Cash Transaction to the EFIC. Ethiopian Banks and Financial Agents are obliged to report all cash deposits or withdrawals and remittances exceeding or equal to Birr 200,000.00 or 10,000.00 USD or its equivalent in other foreign currency. In this scenario, CTR only involves withdrawal or deposits of the minimum threshold without regard to the objective or source of transaction.

[9] Payment Ordered System (POS) is the banking system used for e-commerce by debiting the customer account and crediting the service delivery entity. POS is used by Gas Stations and Supermarkets.

Reporting would facilitate the detection of predicate offences, increase the costs of money laundering and consequently prevent and/or reduce crime.

Therefore, STR and CTR must be supported by an automation of technological tools to report to FIC. Based on correct analysis the report of Ethiopian Banks and Financial Agents about suspected financial transactions could lead to measures to suspend a given account to abort the plot of money laundering. To that end, EFIC is responsible to receive the data and make due scrutiny so that competent authorities would take informed countermeasures.

Anti Money Laundering by its very nature requires international cooperation among countries. Having all rounded cooperation framework helps to cease money laundering in local financial system because money launderers are always searching for countries with careless AML rules or limited international cooperation government. Because of this trend countries like Ethiopia should understand and customize The Forty Recommendations on Money Laundering. In this regard, a rigorous application of Information Technology is critical for seamless automation of AML and for satisfactory implementation of recommendations in Ethiopia.

Chapter Three: Related Work

This Chapter deals with research works that are related to this study. The Chapter is organized into five sections excluding summary of the related work: knowledge based Anti Money Laundering, Ontology based expert system for suspicious transaction, Money Laundering Detection using synthetic data, Fast Detecting Suspicious Money Laundering and An investigation into Data Mining Approaches for Anti Money Laundering.

3.1 Knowledge-based Anti-money Laundering

Knowledge-based anti money laundering is a software agent bank application [25] first developed to control money laundering and is currently in use among financial institutions to handle complex financial transactions and services, including ML. Knowledge based AML which can be used by intelligent agents in a single bank. Intelligent agent is nothing but a computer system in a bank designed to flexibly and autonomously perform activities to meet specific objectives where flexibility includes properties such as autonomy, social capability, reactivity, and pro activity. Intelligent agents can collaboratively deal with complex problems and vast information in dynamic and unpredictable environments.

Knowledge based AML through computer intelligent agents is possible because the agents are versatile with strategies and rules governing business so that actions taken against ML can be justified on legal grounds. In other words the schema with which intelligent agents function monitoring, diagnosis and reporting activities of ML is compatible with a given business law or organizational culture. For instance, intelligent agents detect transactions made by customers in Sanctions list or with controversial background as potential ML activity. Likewise, accounts, and transactions made with that account, with wire transfers but lacking clear business are detected as high ML risks. However, intelligent agents are not concerned with every detail in transactions since the strategy is to focus on critical components such as client ID, transaction type, transaction date, value data, counter party, etc. The interest to diagnosis and reporting by intelligent agents are: transactions with cash value at or above a certain figure (i.e., large amount transaction); transactions with a special transaction type (i.e., high-risk transaction types defined by FATF, such as wire transfer); transactions with a special counter party (i.e., high-risk customers and business entities, like casino owner or somebody from high-risk countries); and transactions of certain frequencies (i.e., high frequency transactions suggest high-risk customer behavior).

Knowledge based AML intelligent agents work in the framework of multiple agents to combat the complex nature of the problem. Although the system is integrated with the entire banking and other financial establishments, it does not interfere with the usual business activities. The Data collecting agent is responsible to collect transaction data based on which to monitoring agents track on the transaction processes. To materialize the multi agent AML framework, the researchers built a prototype in Java so that agents can run on heterogeneous platforms and make use of lightweight applets as temporary agents. But, for prototype evaluation purposes, they used a number of real-world ML cases. The moment ML scheme is detected, the diagnosing agent initiates identification of the problem. The overall AML structure of intelligent agents is depicted in Figure 3.2 [25].

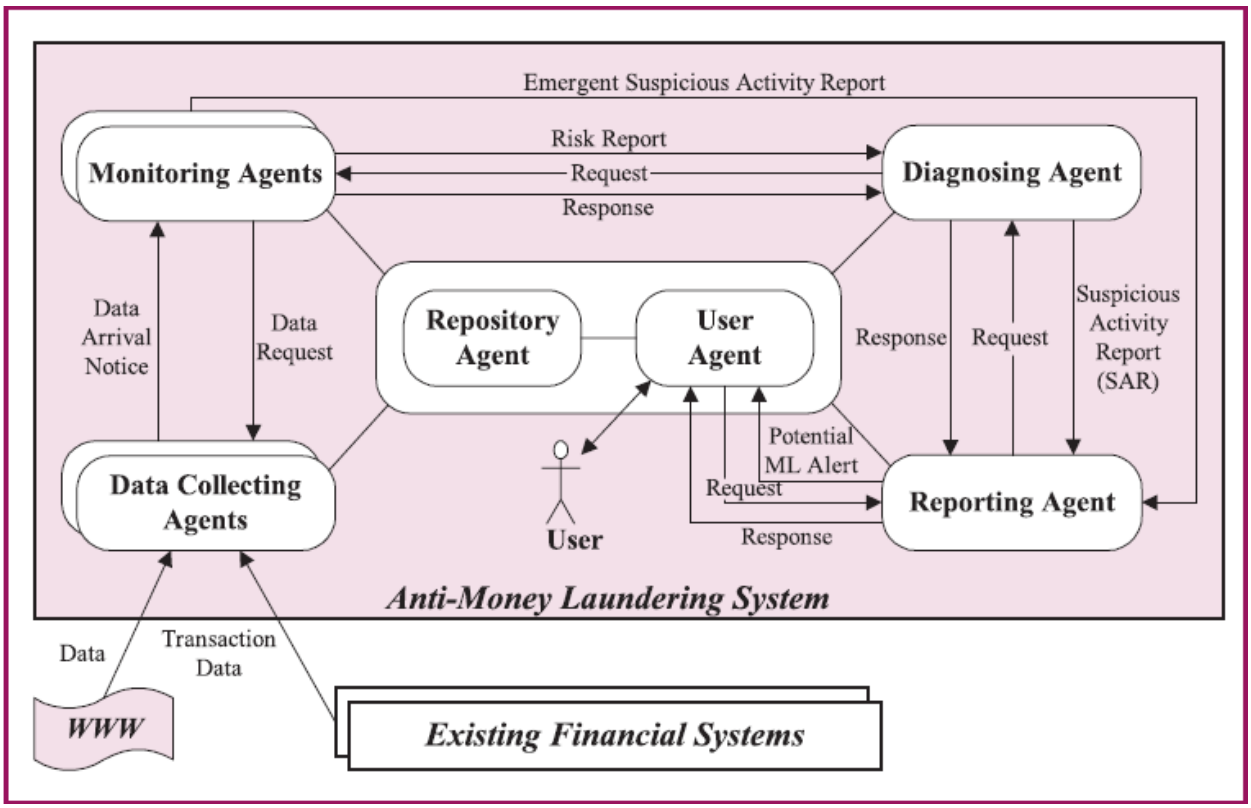


Figure 3.1 : Multi Agent Framework for Anti Money Laundering

Figure 3.1 shows AML platform that focuses on internal data monitoring in a bank, but incapable of monitoring multi-bank transactions. Even though this is the weakness for the research, the Ethiopian banks with their branches supported by proposed software framework which handles multi-bank transactions.

3.2 Ontology Based Expert-System for Suspicious Transactions Detection

Ontology Based Expert-System for Suspicious Transactions Detection [26] is essential for development of AML software. Because computer science researchers adopt similar standards in their fields of study, the ontology of AML has become sharable and reusable. This has led to the development of expert system AML in which the knowledge based and rules based modeling is integrated to detect suspicious transaction detection. Ontology construction, Ontology reasoning and Query on inferred ontology are the three essential components of the expert system. Ontology Construction includes domain knowledge and rule construction which is done after eliminating noisy data through the stage of pre-processing data. Data pre-processing involves: avoidance of irrelevant data related to transactions below the threshold of Money Laundering guidelines, grouping data (based on amount, date, mode of transaction-debit or credit) and determining frequency of transaction and account status (active or dormant).

Ontology Construction relates to establishing the pattern of customers' transactions based on the computation of behavior in the pre-processing stage so that any deviation from the established pattern implies suspicious activity. Establishing a customers' pattern is carried out using Web Ontology Language (OWL) such as class hierarchy, data type properties, object properties, domain range restrictions of each property and instances. Rule construction is the other scene for Ontology Construction which is presented in Semantic Web Rules Language (SWRL) to identify suspicious transactions. Based on the anti money laundering guidelines the rules for large amount, threshold, dormant account, frequent and mode of transaction should be examined and written into SWRL.

The second component is Ontology reasoning, which is applied on the new transaction records. Ontology reasoning is the process of deriving new knowledge that is not explicitly expressed in the initial formulation of customers' behavior, using in-built reasoning engines called Pellet reasoning engine. The inference engine infers the class membership as deduced by the rules and populates the Suspicious Transaction class hierarchy. The last component is Query on inferred ontology which can be performed using SPARQL- the standard query language to query ontology. The SPARQL query displays suspicious transactions. The system was tested using multi million bank data taken over a year and resulted in a two percent suspicious transaction. Both suspicious and non-suspicious transactions are the input for the system and the system does not automatically validate suspicious transactions before applying the rules to detect it.

Validation of suspicious transactions is the weakness of this research. In proposed framework the suspicious transactions are validated using incidence identification and surveillance of ML processes in individual transactions.

3.3 Money Laundering Detection using Synthetic Data

Researchers analyzed the implications of machine learning techniques to detect money laundering. To do so, they used a set of supervised algorithm generated synthetic data from a company providing mobile phone financial transactions [27]. The system was developed to combat ML encountered in three levels of transactions: normal, suspicious and misclassified as anomalies. The researchers used IDAS data and scenario generator tool to generate synthetic data based on the relationship between customer attributes and their statistical distributions. Besides, they adopted Gao's [28] work about AML terms like legal transaction, usual transaction, unusual transaction, suspicious transaction and illegal transaction. The method proved effective in successfully distinguishing high True Positives from law False Positives.

Next to learning the problem is data pre-processing which includes data cleaning and adding some necessary attributes like Customer ID, Profile, Date of the Transaction, type of transaction Amount of the Transaction and city. Once the attributes are formulated, data is labeled anomalous if the amount of withdrawal and deposit is too large or small relative to predefined threshold then drops the small amounts transactions and uses too large amount transactions. Synthetic data was used to train the classifier and test the improvement of detection rate (True Positive) and reduce the misclassification rate of benign data (False Positive). The possible algorithm for detection is analyzed based on Decision Tree Learning and Clustering Techniques.

Decision Tree learning algorithm for the domain of mobile money AML is the possibility for an investigator to determine common rules that classify suspicious behavior. Besides, Clustering Techniques such as distance and density based detection were implemented but it is difficult to find abnormal behavior of the clusters. Due to the lack of real data in this work they used synthetic data, which is important to analyze class imbalance or class overlap proposed by the research. But using synthetic data has its own impact on the research. So that the researcher proposes Multi agent based simulation. One of the main drawbacks of this research is generating the synthetic data which might not represent the real data. And the output from machine learning would bias to use as an output.

3.4 Fast Detecting Suspicious Money Laundering

Le-Khac introduced fast detection of suspicious money laundering [29]. In order to develop a new solution for international investment bank, they proposed a data mining-based solution for AML. In this work they focused on heuristics approach to improve the performance for this solution. Getting money laundering pattern is one of the goals of this research and important to support AML software. Data mining techniques are best suited for identifying trends and patterns from large datasets from banks. According to the researchers perspective all previous works regarding ML and data mining have poor performance which can be improved through clustering approach basing on some heuristics from AML experts.

They considered that only the maximum (redemption) and minimum (subscription) transactions are important to calculate suspicious transaction. But they divided transaction datasets into two: individual and corporate, although they focused on the corporate datasets. Then they applied a two-step procedure: suspicious screening and clustering process. Suspicious screening is the process of taking suspicious data from the whole data set while center based clustering technique is applied for simplicity and effectively. Applying heuristics in suspicious screening process is done by changing the parameters as many times as possible to determine the suspicious group using clustering algorithm. Suspicious and non-suspicious groups are then fed into a neural network for training and their results are stored in a knowledge-base. The drawbacks of this work is classifying the transactions and taking only corporate data. But there exist ML cases from the individual transactions. So that the proposed framework recommended finding suspected transactions from both corporate and individual transactions.

3.5 An investigation into Data Mining Approaches for Anti Money Laundering

The research in [23] seeks to develop a data mining framework for Anti Money Laundering by generating rules and models which are useful for business performance and creating patterns. In addition, the framework helps to investigate money laundering activities. Banking and financial institutions use two kinds of data, one is the archived and stored as historical data and the other is live transaction data. Both archived and live transaction data handled daily and becomes too huge. The process of customer transaction details in individual level is quite difficult. Managing and analyzing effectively this transaction data upon the request using traditional way is much beyond human capacity. Moreover traditional investigative techniques and approaches are labor-intensive and consume numerous man-hours. Definitely, the daily volume of banking

transactions has increased in various ways daily which means that approaches need to be supported by automated tools for detecting and investigating money laundering's pattern.

Accordingly, this research work is motivated to show how data mining techniques should be applied successfully in AML through developing an AML solution based on Data Mining.

Data Mining Prediction can perform different techniques of clustering, classification, regression, association rule discovery and sequential pattern discovery. AML task involves the detection of unusual behavior of all dimensions in transactions, accounts, product types, etc.

In AML, from data mining clustering is normally used for grouping transactions of accounts into clusters based on their similarities of their features transaction types. This technique helps in building patterns of suspicious sequence of transactions and detecting risk patterns of customers holding accounts.

Above all the researcher observed that there are challenges in implementing data mining framework to investigate money laundering. Data quality, data volume and heterogeneity of data and the nature of ML are the main challenges to use the framework. To improve the data quality issue there must be data mining preprocessing techniques applied. Data heterogeneity and distribution of data in different places, is solved by data mining integration techniques recommendations and implementations. The nature of ML can differ with technological advancement of using financial instruments which is a challenge for all kinds of frameworks and AML solution development.

For the realization of the objectives of this study, the researcher hypothesizes that classification and clustering are the two important mining methods that can efficiently be applied for AML. Furthermore, rule based AML solutions have been replaced by artificial intelligent approach for AML; unsupervised learning with a small set of training data is suitable for building Data Mining based solutions for AML. In order to exploit Data Mining techniques efficiently, they need to be integrated in a framework for detecting Money Laundering. The weak point in this research is because of nature of ML it is difficult to identify ML activities from the transaction data.

3.6 Summary

Anti money laundering policies, procedures and researches not only contribute towards the safety and systematic way of controlling ML but also assist the protection of the integrity of the financial systems.

The multi agent for tackling ML to achieve knowledge-based solution proposed by researchers allows integrating AML techniques with specific knowledge about business rules and business strategies. But it is implementable only in one bank transactions. The other related work belongs to Expert system using ontology which is a good choice for incorporating both knowledge base and rule based modeling. However, the expert system does not automatically validate the suspicious transactions rather it applies the rules to detect suspicious transaction.

Detection of money laundering through machine learning using synthetic data represents an improvement of detection rate (True Positive) and reduces the misclassification rate of benign data (False Positive). However, this system has not been tested for accuracy based on real data. It is, thus, difficult to say about the relative advantages of this research over AML detection using machine learning based on synthetic data. It could, however, be appreciated that this research is a step forward for it integrates the various features of models discussed.

Chapter Four: The Proposed Framework

4.1 AML Software Framework for Ethiopian Banks and Financial Agents

The main objective of this work is designing a SW framework to control ML for Ethiopian Banks and Financial Agents. Figure 4.1 shows high level AML Software Framework for Ethiopian Banks and Financial Agents.

The framework is classified in to three parts according to the framework implementation areas. AML software framework can be implemented into banks and agents, NBE and FIC.

There are three framework components which can be implemented at banks and agents.

- KYC schema
- Data submission module
    - Cash Transaction Data
    - Suspicious Transaction Data

There are two framework components that can be implemented at the NBE.

- NBE Remittance Monitoring System
- NBE Cash Data Validation System

There are two framework components and one framework report which can be implemented at FIC.

- Cash Activity Process Model
- Suspicious Activity Process Model
- Detection Avoidance Report

Each of the framework components, systems and models are demonstrated in their sections.

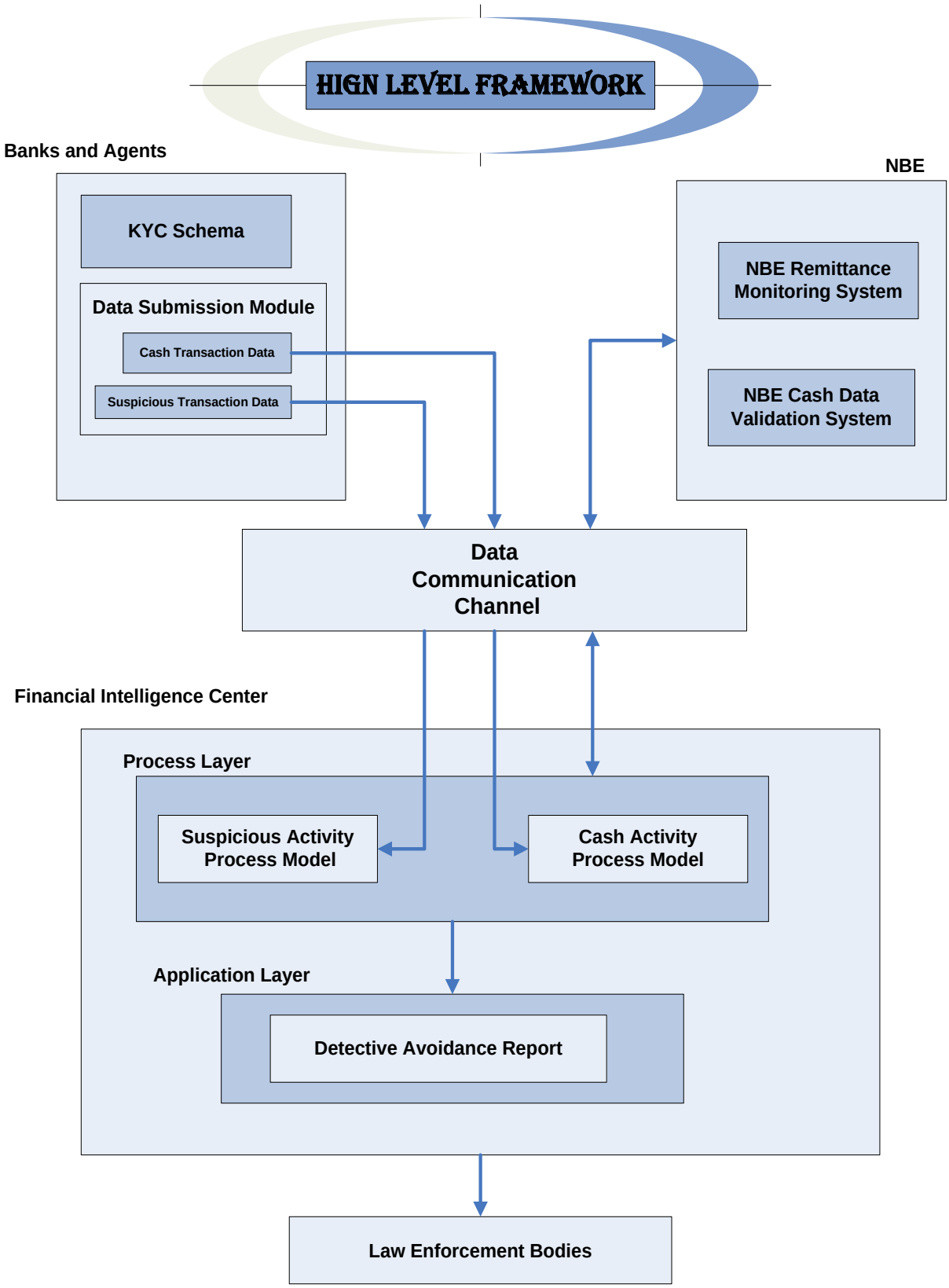


Figure 4.1 : AML Software Framework for Ethiopian Banks and Financial Agents

4.2 Know Your Customer Schema

Know Your Customer (KYC), which is the licensing and supervision of banking business by National Bank of Ethiopia, is a directives created for customer due diligence of banks directives [22]. Since KYC is the first way of controlling money laundering therefore banks should know their clients before they become customers of the bank. The proposed software framework has its own KYC schema as shown in Figure 4.2.

KYC schema is the data communication between banks and financial intelligence center through the Internet.

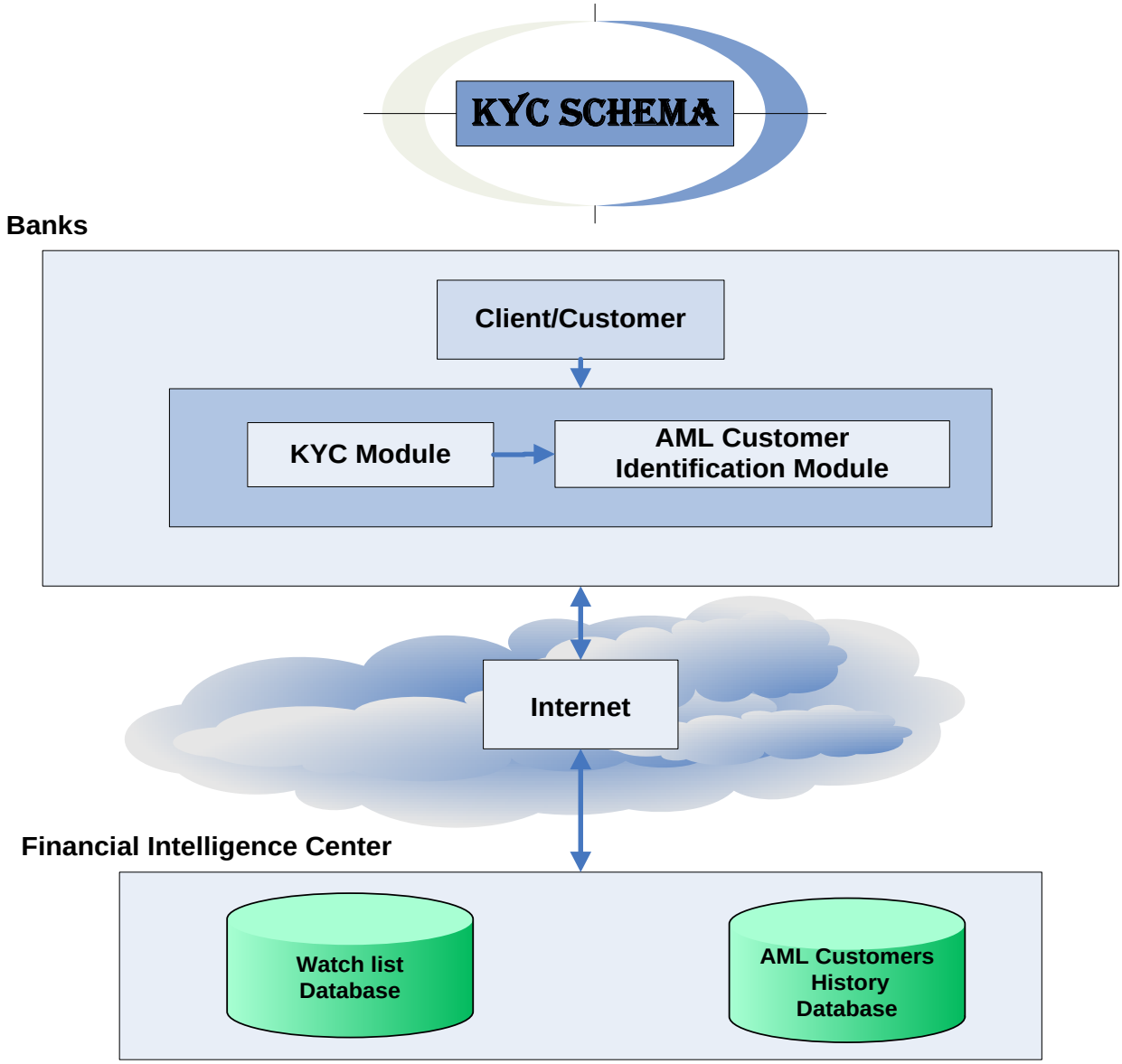


Figure 4.2 : KYC Schema

Delinquent list is the register held by NBE and disseminates to all banks which indicates the names of current account holders whose cheques have been dishonored and accounts are closed by banks for security reasons. An insufficient balance is one of the dishonored activities. Checking the current account customers from the delinquent list should be included in KYC procedure. Figure 4.3 shows the KYC Module and AML Customer Identification flow chart.

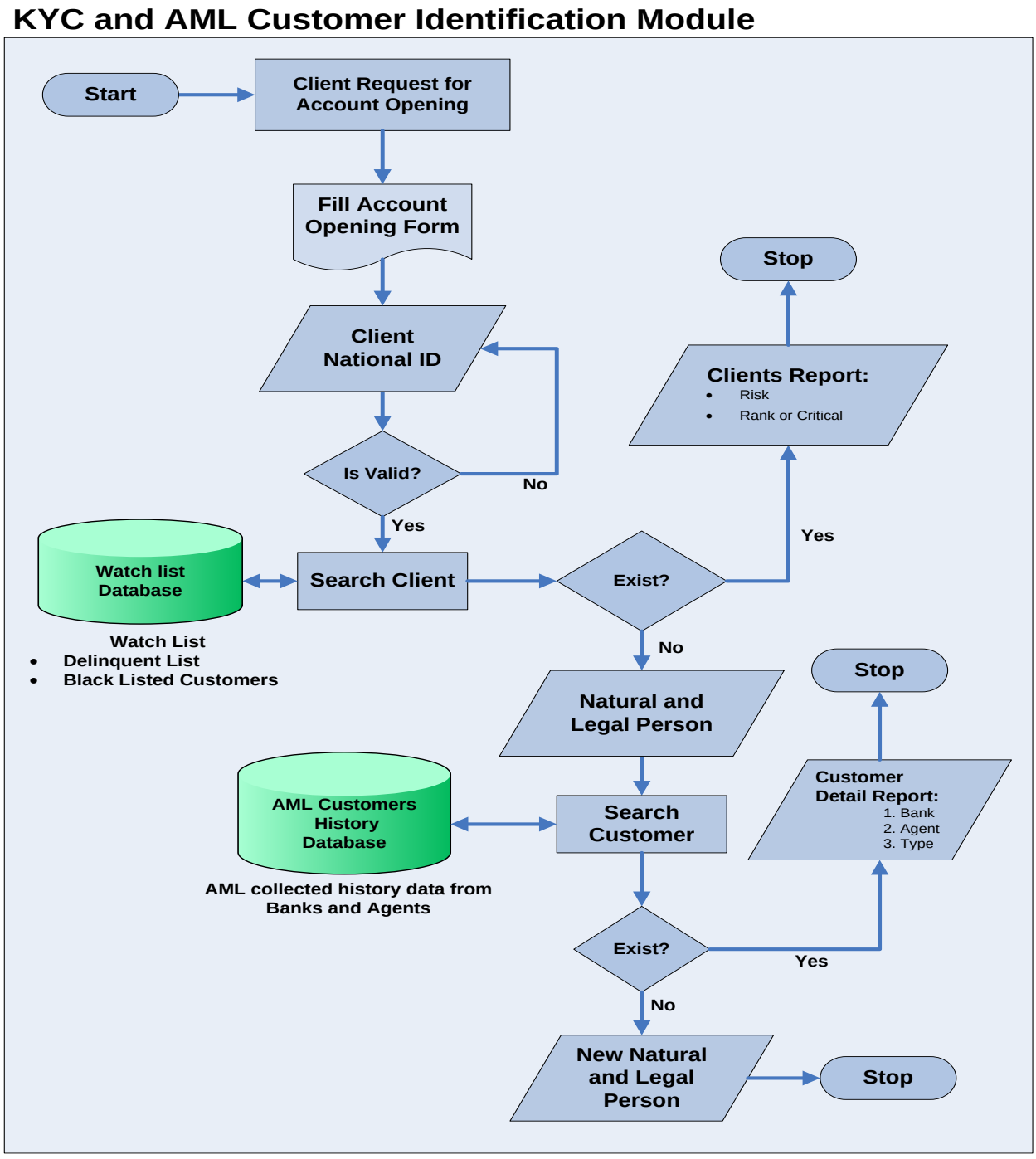


Figure 4.3 : KYC Module and AML Customer Identification module flow chart

4.2.1 KYC Module

KYC module is used to know your customer and checking who the client is. Once the clients presented in the bank within the relevant documents to open an account, the bank should know the clients from watch list database which resides on FIC through the web application. The watch list database contains black listed customers and delinquent list from all banks those are registered in delinquent list. National ID for individuals suggested in this work is used to know the customer activity from watch list database which is important to understand who the client is. If the client is free from delinquent list then he/she can be legal and natural person to process any kind of banking activities otherwise the bank should not start any activities with this client. According to [22] directives "Legal person" refers to a body corporate, foundation, partnership, non-profit organization or association, or any similar body that can establish customer relationship with a bank or other financial institution, or otherwise own property.

4.2.2 AML Customer Identification Module

AML Customer Identification is the process identifying whether the customers exist in the history of AML cash or suspicious transaction activity. Legal person should be checked from AML Customers History Database to identify the true identity of the customer, ownership and beneficial of the account, funds source, the nature of customer's business and reasonableness of operations in the account of one's business. If the client is free from both, then he/she can be new legal person. The report output from this process of AML Customer Identification is displaying about the customers details for the banks.

4.3 Transaction Data Handling

There are two types of transaction data handling in banks and financial agents: cash transaction data and suspicious transaction data handling.

4.3.1 Suspicious Transaction Data Handling

Suspicious transaction data handling is the way for handling of suspicious transactions data and makes ready the data for sending as suspicious to the Ethiopian Financial Intelligence Center. The process of suspicious transaction data handling includes suspicious cash and remittance data entry in the way of single transaction entry or multiple transactions entry. This will be implemented in Banks and Financial Agents to submit data to the FIC database.

A) Banks

Banks are the main data source for suspicious transactions so that they can handle the data using the system which supports for collecting and organizing the suspected transactions. There are two kinds of suspected transactions that can be handled in the banks. These are Suspected Cash Transactions and Suspected Remittance Transactions. Figure 4.4 shows classification of banks suspected transaction. Both Suspected Cash Transactions and Suspected Remittance Transactions are one of the problems of Money Laundering.

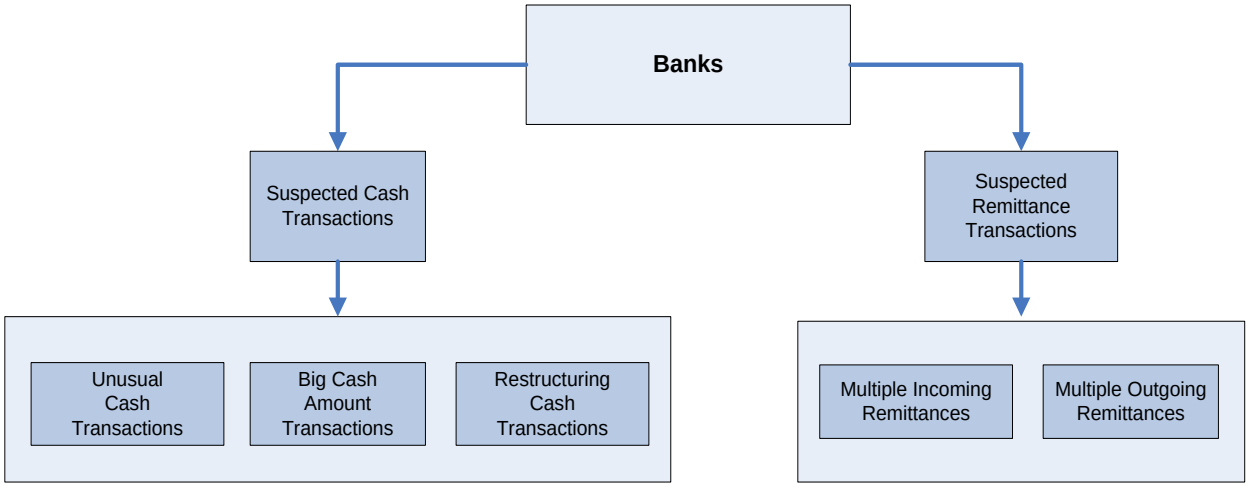


Figure 4.4 : Banks Suspected Transaction Classification

i) Suspected Cash Transactions

Suspected Cash Transactions are processed for the customers using their bank passbook if they used saving accounts category or if they used cheque for their accounts belonging to the current account category. If the transaction amount is equal to or above the limit which is recommended by NBE in customer due diligence of banks directives, it is reported as cash transactions but if it is less than the limit within some situations, it becomes suspected cash transaction. Suspected cash transactions are classified in to three parts. These are Unusual Cash Transactions, Big Cash Amount Transactions and Restructuring Cash Transactions.

- **Unusual Cash Transactions**

Unusual Cash Transactions occur when usual transactions happen repeatedly for long period of time but there happens a sudden change of quite different transaction in amount occurs then we say it is suspected cash transaction. For instance if the customer is an employee of a government office, and he/she earns a salary and process his/her salary transaction but if he/she unusually deposit or withdraws more than the specified limit amount then the transaction becomes unusual

and it becomes suspected cash transaction. The limit amount is determined as the same as NBE directives which is the same as Birr 200,000.00 or 10, 000.00 USD (or equivalent to this amount in other currencies).

- **Big Cash Amount Transactions**

This is the case in which the bank customer processes the number of transactions in the bank for long period of time within some interval amounts but in some cases the customer might process the very big amount of transaction so that at this time this big amount transaction becomes suspected big cash amount transaction. For instance the customer processed the transactions not more than Birr 500,000.00 for the last three months and then the customer tries to process Birr 2,000,000.00 in other time which tells us this transaction is big suspected cash amount transaction and reported immediately to FIC office.

- **Restructuring Cash Transactions**

There is a customer who wants to process the big amount transactions by break down or structuring the transaction to small amount transactions, which is the amount below the Birr 200,000.00. The bank should structure or sum the amount of the customer transaction repeatedly much many times as possible, to get the total amount above or equal to the threshold amount. Therefore the bank compliance officer should restructure the transactions based on the customers to find restructure cash transactions of the bank.

ii) Suspected Remittance Transactions

Banks are working remittances in local currency throughout the country and in foreign currency remittances outside of the country using financial agents. Therefore there are transactions beyond or equal to Birr 200,000.00 which is reported as remittance transactions but in some circumstances the remittance transactions become suspected. Suspected Remittance Transactions are classified in to two types. These are Multiple Outgoing and Multiple Incoming.

- **Multiple Outgoing Remittances**

There are conditions for sending of remittances to a number of different persons in the same city to the same person to different cities. But in all cases the originating branch is the same, at this time it is called multiple outgoing remittance.

➢ **Multiple Incoming Remittances**

Multiple incoming is the process of receiving remittances from a number of clients or customers through the agents or banks. The sender might be the same or different individuals from the same or different cities but the receiver is the one who is legal or illegal person who is the beneficiary of the remittance. At this time the beneficiary transaction becomes multiple incoming suspected remittances.

B) Financial Agents

Financial Agents are also the source of suspected transactions which is collected from remittance data of the customer. The remittances performed by the Financial Agents are coming from abroad that is the sender is always outside of Ethiopia while the receiver or beneficiary is in Ethiopia. There are three kinds of suspicious remittance transactions. These are Unusual Remittance Transactions, Big Amount Remittance Transactions, and Multiple Incoming. Figure 4.5 shows Financial Agents Suspected Remittances classification.

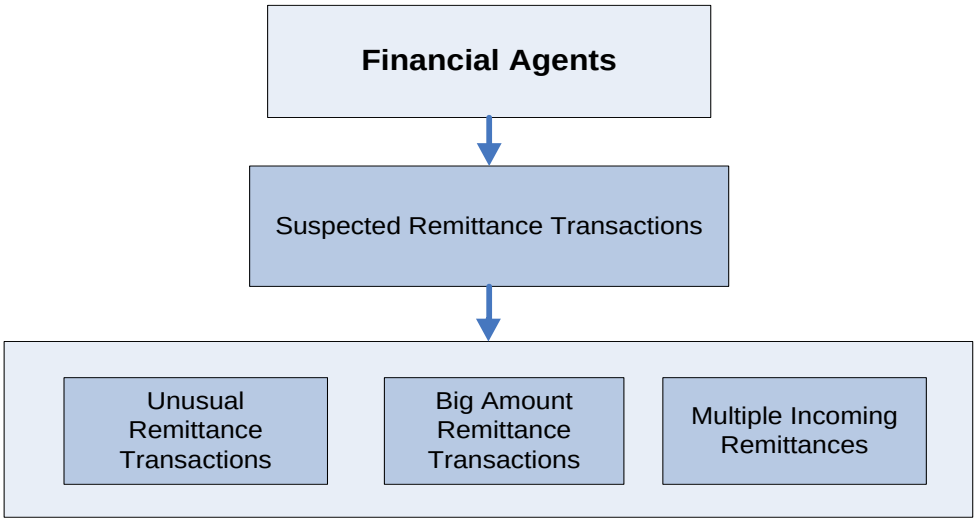


Figure 4.5 : Financial Agents Suspected Remittance Classification

➢ **Unusual Remittance Transactions**

Unusual remittance transactions are similar to the Unusual Cash Transactions except it is the remittance processing in an agent's office rather than cash transactions processing in the bank. For instance if the address of the sender not be fully described in the remittance which shows that they tried to conceal the source of fund and the remittance transaction becomes unusual and suspected.

- **Big Amount Remittance Transactions**

If the customer is processing big amount of remittance, then it can be taken as suspected remittance transactions. For instance the beneficiary requests the amount above 20,000.00 USD or equivalent in other currencies. This transaction needs to be reported immediately as big amount remittance transaction to FIC. Because of the agents does not have permanent customers for processing the transactions.

- **Multiple Incoming Remittances**

Multiple incoming remittances in agents are similar to multiple incoming local remittances in banks what we have seen previously. This is the process of receiving remittances from a number of clients or customers from abroad to Ethiopia through the agents.

4.3.2 Cash Transaction Data Handling

Cash transaction data handling is the process of handling cash transaction data in banks and financial agents' transactions amount greater or equal to Birr 200,000.00 or 10,000.00 USD or equivalent in other currencies. Therefore it is necessary to handle the data which are processing by the banks or financial agents based on this amount.

We have seen that the transactions within this amount recommended by NBE customer due diligence of banks directives must be reported from any bank or agent to the EFIC. There are three kinds of cash transaction data that should be handled. These are Cash Withdrawal, Cash Deposit and Remittances. The overall cash transaction data in handling process classification is shown in Figure 4.6.

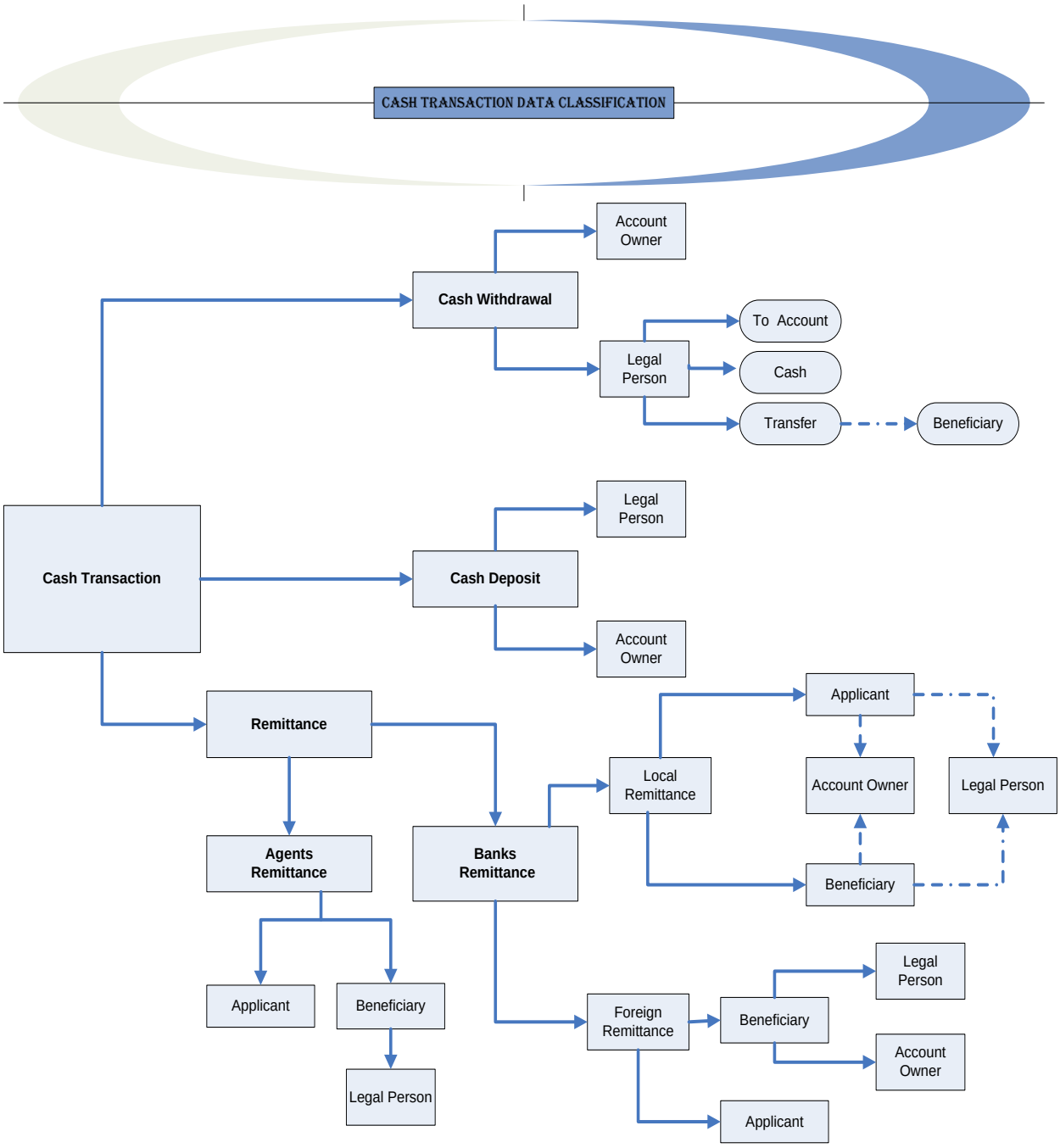


Figure 4.6 : Cash Transaction Data Classification

i) Cash Deposit Transactions

Processing Cash deposit transaction at the minimum or exceeds Birr 200,000.00 or 10,000.00 USD or equivalent in other currencies is initiated either by the account owner or any legal person. In both cases the accountability belongs to the person who initiates the transaction must be identified and reported to FIC.

ii) Cash Withdrawal Transactions

Any cash withdrawal transaction is processed by the account owner where the account owner stands in front of the bank teller. And the other cash withdrawal can be performed by the legal person the one who receives the financial instrument from the bank customer or account owner. Therefore in both cases it is necessary to identify the beneficiary as account owner or legal person. The legal person can withdraw the money in three different ways from the Ethiopian banks. He/she can transfer the amount to his/her account, withdraw in cash, or transfer to any other beneficiary. In all three cases the legal person or the beneficiary should be identified.

iii) Remittances Transactions

Remittance is the money transferring method from one place to another, where the applicant is the sender of the money and beneficiary is the receiver of the money. This remittance can be processed by banks or agents.

A) Agents Remittance

All financial agents in Ethiopia are working in money transfer from abroad to Ethiopia. In agent remittance the assumption is the applicants are living in other countries and the beneficiary is in Ethiopia. The beneficiaries in financial agents or banks are legal persons and should be identified. From the applicant side the only information required is the country of the sender and sender bank if exists should be identified.

B) Banks Remittance

There are two types of remittance transactions processed by the banks differentiated by the location, Local Remittance and Foreign Remittance.

i) Local Remittance

Local remittance is the one which initiates from any town of Ethiopia and process through the banks. Both applicant and beneficiary can be the account owner of the bank or legal person. In all cases the applicant and the beneficiary should be identified for local remittance transactions.

ii) Foreign Remittance

Foreign Remittance in banks is the money transfers from other countries to Ethiopia through the banks or their branches. The same as remittance in agents stated above the applicant country and

sender bank if exists should be identified. The beneficiary can be a legal person or bank account owner. Therefore it is necessary to be sure that the beneficiary should be identified.

4.4 Data Submission Module

Transaction data should be submitted from banks and financial agents to EFIC through the web application. Once the transaction data are handled then it is necessary to submit to EFIC for further analysis and investigation. Banks and financial agents extract their data from their legacy system and after validation and data conversion using data submission module they submit their data to EFIC database. The process of how the data can be submitted to EFIC as shown in Figure 4.7.

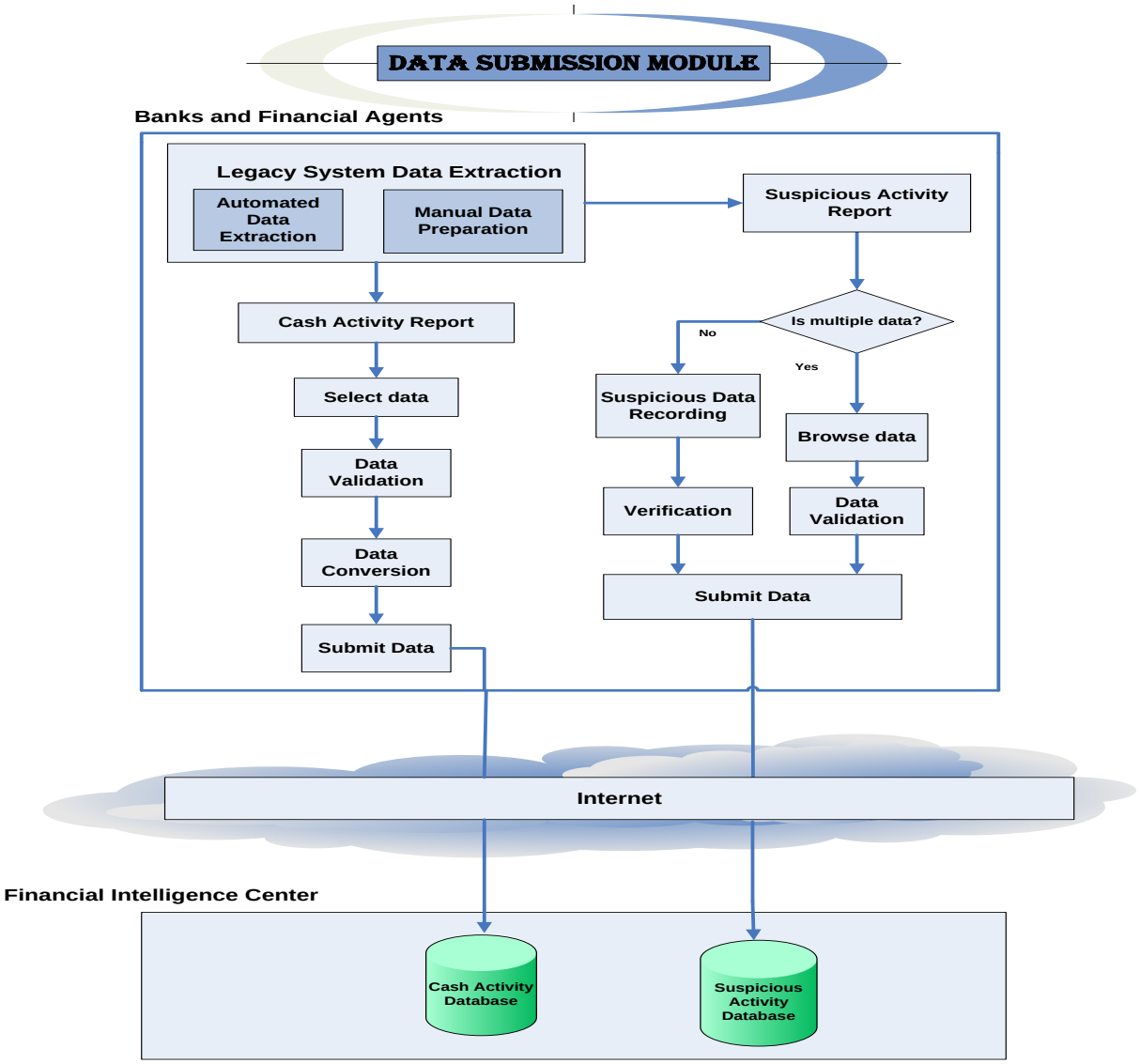


Figure 4.7: Data submission module work flow

4.5 Data Submission Module Algorithm

Data submission module algorithm serves as insertion of data into database. The algorithm accepts data file like excel, text file, so on or input data from keyboard as an input and submitted to the database, which do not return any output. This algorithm used by both Cash and Suspicious Data Handling systems.

Algorithm 4.1: Data Submission Module Algorithm

```
1. Input
       Excel file or CSV file or text file
       Input Fields data
2. Set variables
       Set DataFile<> is null
     // create empty list to hold data file
       Set InputData<> is null
     // create empty list to hold input data
       Set EntryMode is null
     //set empty to the entry mode
       Set DataContext is null
       Set DataFields<> is null
     // create empty list to hold fields data
       Set validDataType is null
3. EntryMode ← Select the Entry mode
4. If EntryMode is single Then
     DataFields ← Input Fields data
     checkedData ← CheckDataType(DataFields)
        If checkedData then
             Submit (checkedData) →datatable
        End if
       Else     // entry mode for  multiple data
            InputData ← Validate(DataFile)
            // validate the input file before process
       End If
```

```
5. InputData ← Validate(DataFile)
      DataFile → DataContext
      // copy datafile to the data context
      For every row element of DataContext endRow
      validDataType ← checkDataType(DataContext)
             If validDataType Then
               Next
             Else
               Return
             End If
      End for
6. validDataType ← checkDataType(DataContext)
      fileToCheck ← DataContext
      For every row element of DataContextendRow
             If fileToCheck  Then
               Return validDataType
             Else
               Display_message("Incorrect Data Type ")
             End If
      End for
7. For every row element of DataContextendRow
         Submit (DataContext) → datatable
  End for
```

4.6 Transaction Activity Process Models

The second organ which receives and processes the data from banks and agents is Ethiopia Financial Intelligence Center. The process and model of performing at this organization is called transaction activity process models. In the proposed framework it contains two major layers. One is the process layer which has two major process models and the other is application layer which is the output as Detective Avoidance Report.

4.6.1 Suspicious Activity Process Model

This process model holds the activity of suspicious transactions which is collected from all Ethiopian banks and Financial Agents. The Suspicious Activity Process Model contains two main tasks. These are Incidence Identification and Surveillance of Money Laundering.

A) Incidence Identification

Incidence Identification is the primary step of doing suspicious activity for the process of Suspicious Activity Process Model. The Incidence Identification for the suspicious activity starts from the Suspicious Activity Database. The last output of Incidence Identification process is kept under Suspicious Transaction database. The Incidence Identification process is performed by senior system analyst at FIC office. The four major tasks performed in Incidence Identification are shown in Figure 4.8.

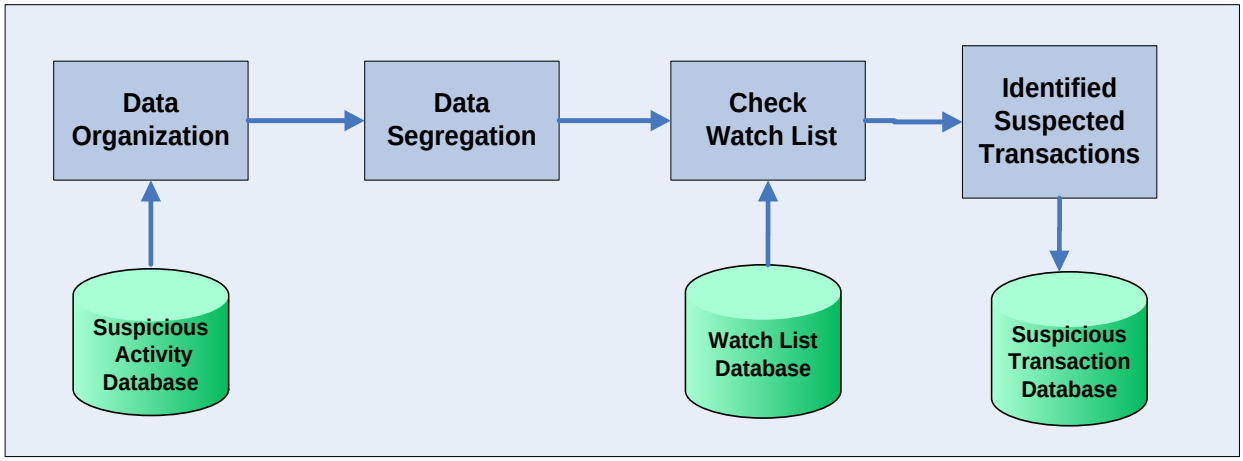


Figure 4.8 : Suspicious Activity Process Model – Incidence Identification

- **Data Organization**

Suspicious Data should be organized in some logical, efficient order which is very important easily to understand. The collected suspicious data organized using duration or order of time, banks and agents.

- **Data Segregation**

First the organized suspicious data segregated by the amount and frequency of transaction. Next the transaction data is isolated not only by amount and frequency but also the city or region of the transaction must be identified for the purpose of summarizing. The transaction segregation by city and region is used for identifying suspicious cash flow.

➢ **Check Watch list**

Before deciding the transaction is suspicious at this step it is necessary to check the related transactions whether performed previously or not from watch list database. This task is important to know the severity of the transaction. Using the National Identification Number or National ID of the customer, suggested in this research, the transaction easily related to watch list database data.

➢ **Identified Suspected Transactions**

The last step of Incidence Identification is submitting suspicious transactions to the database, which is next to the above checking watch list. All data that is related from watch list and unrelated data those are not existed in watch list previously should submit into Suspicions Transaction Database.

B) Surveillance of Money Laundering

Once the transaction is identified as an incidence and submitted to Suspicious Transaction Database the next step will be Surveillance of Money Laundering. The Surveillance of Money Laundering is performed by FIC Senior Investigator. There are four major tasks performed under surveillance of money laundering. These are Filtering and Classification, Investigate Individual Transaction, Case Administration and Submitting Surveillance Result. Figure 4.9 shows that Surveillance of Money Laundering.

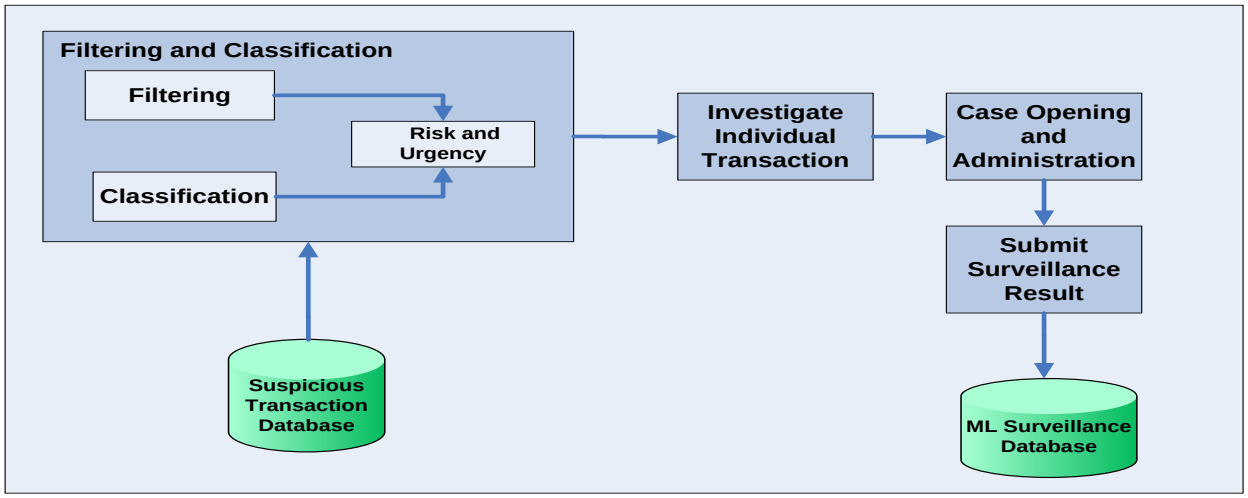


Figure 4.9 : Suspicious Activity Process Model – Surveillance of Money Laundering

➢ **Filtering and Classification**

At this stage the suspicious transactions which is resides on Suspicious Transaction Database filtered and classified by its risk type and urgency. Risk of suspicious transactions classified as

high, medium and law, and similarly urgency of suspicious transaction classified as top urgent, urgent and normal.

- **Investigate Individual Transaction**

Under the investigation of individual transaction the senior investigator identified the transaction detail of each transaction with its customer review. Which includes who initiate the transaction, when transaction initiated, identify if there exist narrative of transaction, how transaction is performed, check the payment instrument and other important input for case opening.

- **Case Opening and Administration**

Once the transaction is investigated then the next step will be opening the case for the transaction and administer the case of the transaction as Money Laundering.

- **Submit Surveillance Result**

The last step of the process is submitting the surveillance result to the ML Surveillance Database.

Finally the Suspicious Activity Process Model has two major tasks as depicted in Figure 4.8 and Figure 4.9. The general Suspicious Activity Process Model shown in Figure 4.10.

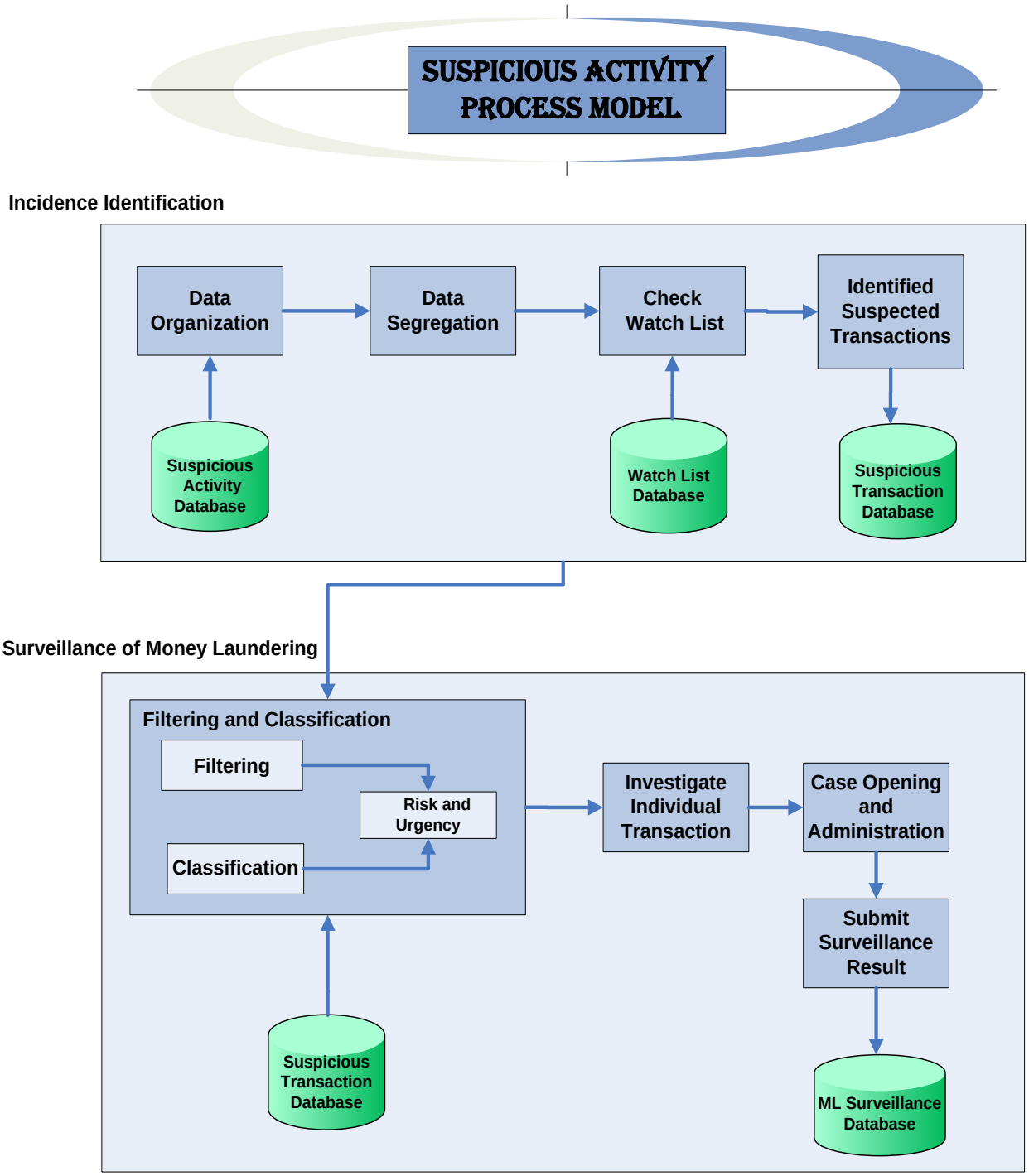


Figure 4.10: Suspicious Activity Process Model

4.6.2 Suspicious Activity Process Algorithms

Incidence Identification and Surveillance of ML algorithms are the two algorithms used by Suspicious Activity Process Model.

A) Incidence Identification Algorithm

Incidence identification algorithm performs filtering by accepting one of the criteria Date, Bank or Agent, Amount, or Frequency. And sort the filtered data by region and city to analyze the cash flow in the region. The sorted data should check against to the watch list from the delinquent list. Then submit the filtered and sorted data to suspicious transaction database.

Algorithm 4.2: Incidence Identification algorithm

```
1. Input
            Date
            Bank/Agent
            Amount
            Frequency
            National ID
2. FilterBy(date, bank/agent) ⟶ datatable

// Call Filter the data from data table using date, bank/agent

3. Set Variables
      Set outputData<> is null
       // create empty list to hold output data
      Set filterData<> is null
      // create empty list to hold filter data
      Set sortData<> is null
      // create empty list to hold sort data
      Set customerDetail<> is null
       // create empty list to hold customer detail
      Set datedatacontext is null
      Set bankagentdatacontext is null
4. outputData ⟵ FilterBy(date, bank/agent)
```

```
5. FilterBy(date, bank/agent)
          Datedatacontext ←— datatable
          bankagentdatacontext←—datatable
      If date is valid and bank/agent exists Then
          For every row element of bankagentdatacontextendRow
              For every row element of datedatacontextendRow
                  Return   filterData←—datedatatable
                   Return    filterData←—bankagentdatatable
               Next For
              Next For
               End for
          End for
      Else
         Display_Message("Invalid date or
         Bank/Agent does not exist")
         Return
      End If
6. SortBy(amount,frequency) —→datatable    //call to sort the
   data table by amount
7. outputData←—SortBy(amount,frequency)
8. SortBy (amount,frequency)
      datedatacontext←—datatable   //return the data table to
      date data context
      bankagentdatacontext←—datatable
      If amount is valid and frequency exists Then
          For every row element of bankagentdatacontextendRow
              For every row element of datedatacontextendRow
                 Return   sortData←—bankagentdatatable
                 Return    sortData←—datedatatable
              Next For
              Next For
               End for
          End for
      Else
```

```
          Display_Message("Invalid amount or frequency does not
          exist")
          Return
        End If
9. checkData←outputData
10. CheckWatchlist (indId, checkData)
    // function for checkwatch list
      //Select indId from checkData
      For every row element of checkDataendRow
       //check for each data context
             If indID exists then
          customerDetail<>←cusomerBank/Agent,type
          display_message(customerDetail<>)
          Else
             Return
          End If
      End For
      customerDetail<>←cusomerBank/Agent,type
      display_message(customerDetail<>)
 11. Update(outputData) ←customerDetail<>
 12. Submit (outputData) →datatable
```

A) Surveillance of ML Algorithm

This algorithm performs filtering and classification by using risk and urgency of the records from the database and returns the individual transaction for investigation and case opening. Once the data is investigated then it is ready for case opening by submitting the result to ML surveillance database.

Algorithm 4.3: Surveillance of ML algorithm

```
    1. Input
            Risk
            Urgency
    2. FilterBy(risk,urgency) ⟶datatable
    3. Set Variables
           Set outputData<> is null
       // create empty list to hold output data
           Set riskdatacontextdatacontext is null
        // create empty data context
           Set urgencydatacontextdatacontext is null
           Set searchDatadatacontext is null
           Set filterUrgencyDatadatacontext is null
        // create empty data context
           Set filterRiskDatadatacontext is null
       // create empty data context
Set customerDetail<> is null
//create data context to hold customer detail
    4. outputData⟵FilterBy(risk,urgency)
      riskdatacontext⟵datatable
      urgencydatacontext⟵datatable
         If date is valid and bank/agent exists Then
             For every row element of riskdatacontextendRow
               For every row element of urgencydatacontextendRow
                    Return   filterUrgencyData⟵datatable
                    Return    filterRiskData⟵datatable
                 Next For
               Next For
             End for
            End for
```

```
      Else
         Display_Message("Invalid risk or
         urgency does not exist")
         Return
      End If
5. outputData←filterUrgencyData, filterRiskData
6. openCase(outputData (txnReference))
7. If txnReference exists then
   customerDetail<>← Search(txnReference)
   display_message(customerDetail<>)
   Else
      Return
   End IF
8. Search (txnReference) → datatable
   Set searchData context is null
      For every row element of searchDataendRow
         If txnReference then
           Return searchData
         Else
           Continue loop
         End If
     End for
9. customerDetail<> ←searchData
10.    Submit (customerDetail<>) →datatable
```

4.6.3 Cash Activity Process Model

One of the core activities of Money Laundering involves in cash activities of the banks and financial agents so that the cash data according to NBE directive is the input for Cash Activity Process Model. The collected cash transaction data resides on Cash Activity Database which is the beginning for Cash Activity Process Model.

Cash Activity Process Model has three major tasks: CAR Data Organization, CAR Data analysis and CAR Case Investigation.

A) CAR Data Organization

Banks and agents are the main sources for Cash Activity Report or CAR. The collected data is organized at the first stage called CAR Data Organizing. CAR Data Organizing has four major tasks. These are Data Organizing, Data Restructuring, Check Watch List and Update Customer Data. Figure 4.11 shows that CAR Data Organization.

- **Data Organization**

All cash transactions data collected from banks and agents are not completely transacted for money laundering it should be organized in some logical, efficient order to easily understand the transaction. The collected cash data organized using duration or order of time, banks and agents.

- **Data Restructuring**

Restructuring is collecting individual customer transactions from different banks or agents by using the date range and National ID of the customer collected into the sum amount.

- **Check watch list**

To predict the cash transaction is suspected as money laundering one of the steps is checking the customer details from the watch list. Therefore after data restructuring step check watch list is followed.

- **Update customer data**

Once the checking watch list is completed then the next step will be updating the customer details on the customer's history database.

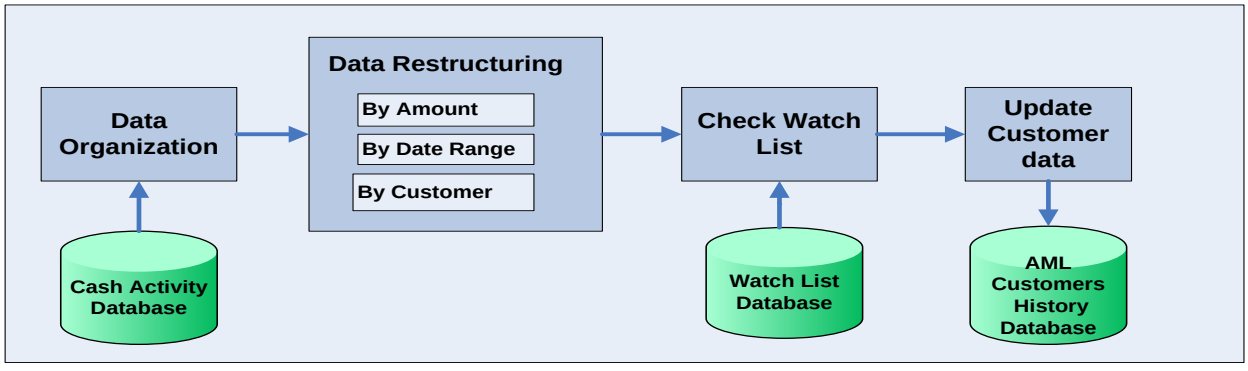


Figure 4.11: Cash Activity Process Model – CAR Data Organization

B) CAR Data analysis

Once the data is organized it is necessary to analyze through analysis method for the purpose of Anti Money Laundering. CAR Data Analysis has four major activities. These are CAR Analysis,

Monitor Individual Customer, Data Filtering and Case Matching. The Figure below Figure 4.12 shows that CAR Data Analysis.

- **CAR Analysis**

From the list of cash transaction CAR Analysis task includes the analysis of customer transactions with its frequency, amount and classification. Classification of customers is always depends on the source data collected from banks and agents.

- **Monitor Individual Customer**

The output of CAR Analysis shows that the details of the individual with related transaction, so that it should be monitored the individual customer at this step.

- **CAR Data Filtering**

For the selected customer transactions filter individual transaction data by amount, date and institution, where and when the transaction is processed, to make ready for case matching.

- **Cash Transaction Case Matching.**

The request on individual customer transaction has collected manually from law enforcement bodies and needs matching with collected data from banks and agents. Cash Transaction Case Matching is the task of matching the manual data and the analyzed individual customer data.

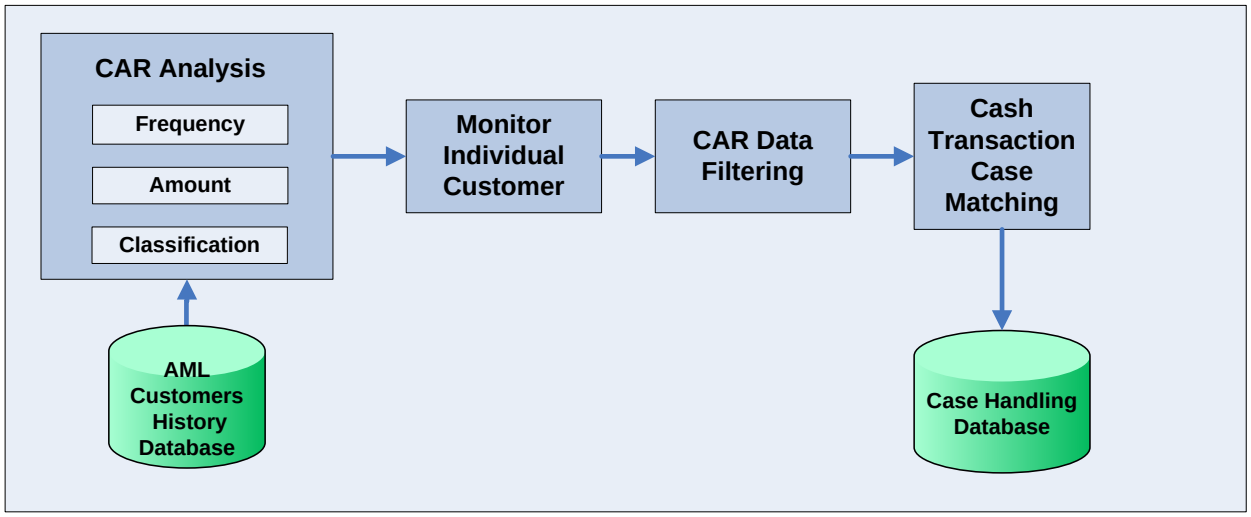


Figure 4.12: Cash Activity Process Model – CAR Data Analysis

C) CAR Case Investigation

After the Cash Activity analysis the next step is investigating the cash transaction. There are five major tasks performed under CAR investigation. These are Case Opening, Case Analysis, Case

Investigation, Case Review and Cash Activity Detective Avoidance. The Figure below Figure 4.13 shows that CAR Investigation.

- **Case Opening**

For the individual cash transaction selected suspected transaction and case opening is the first step for the investigation. Using individual national ID case will be opened to investigate the transaction.

- **Case Analysis**

Case analysis is the task of analyzing the case using case analysis methods for the opened cases.

- **Case Investigation**

Before deciding the transaction processed by customer as money laundering the case investigation team has investigated the customer's history with transactions.

- **Case Review**

The case report is prepared and necessarily case is reviewed and approved for next Detective Avoidance.

- **Cash Activity Detective Avoidance**

Cash Activity Detective Avoidance is the final decision of the transaction which is registered on Detective avoidance database.

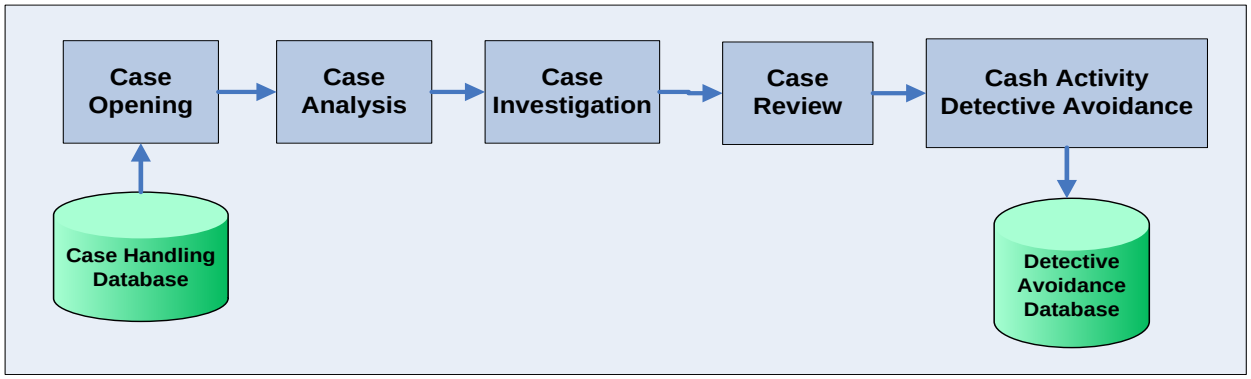


Figure 4.13: Cash Activity Process Model – CAR Data Investigation

Finally the Cash Activity Process Model has three major tasks and depicted above in Figure 4.11, 4.12 and 4.13 and the general Process Model of cash activity as shown in Figure 4.14.

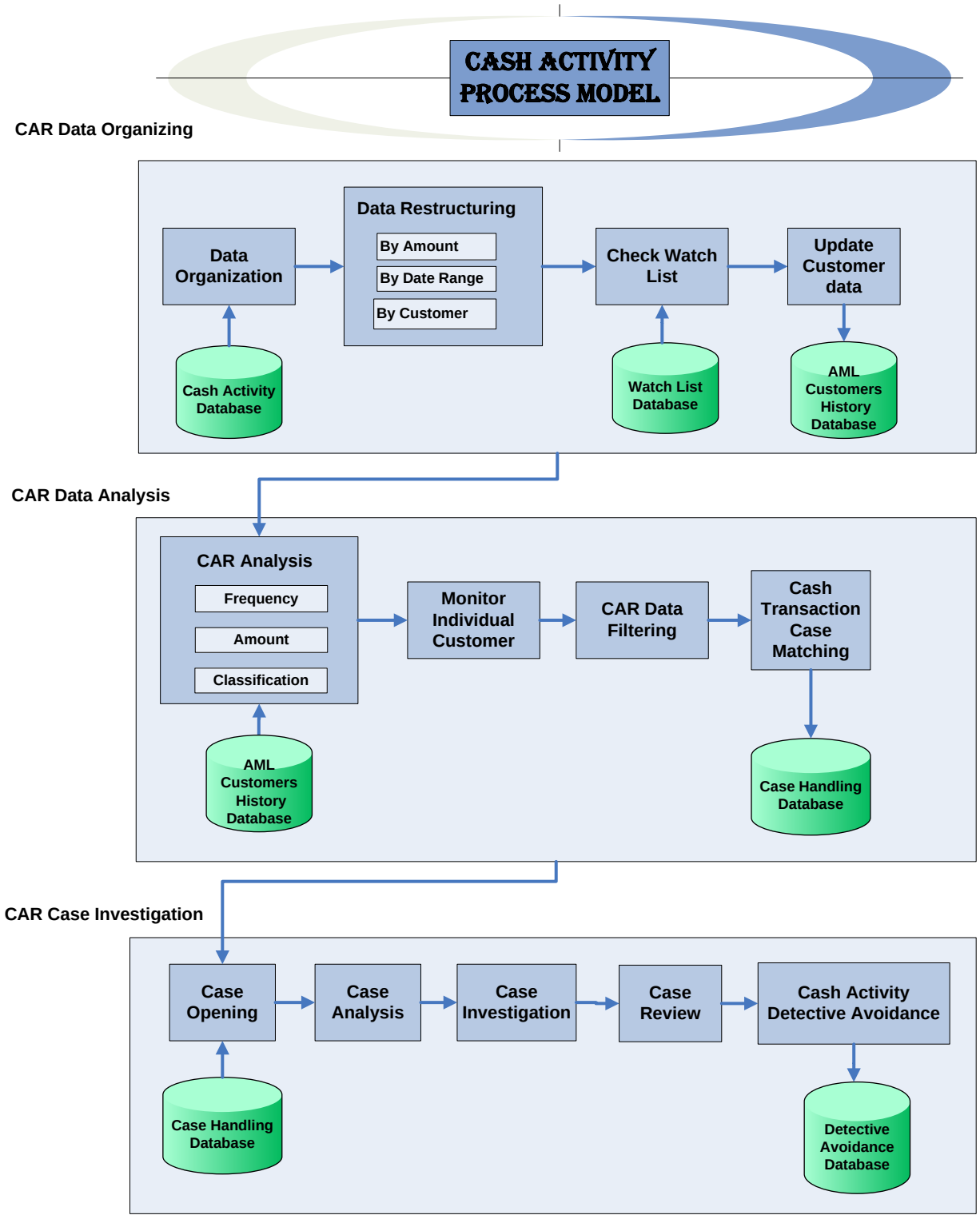


Figure 4.14: Cash Activity Process Model

4.6.4 Cash Activity Process Algorithms

There are three algorithms used by Cash Activity Process namely CAR Data Organizing Algorithm, CAR Data Analysis Algorithm and CAR Case Investigation Algorithm.

A) CAR Data Organizing Algorithm

Cash Activity Report Data organizing algorithm accepts date and bank or agent to organize the data table of cash transaction collected from banks and agents according by the given date and bank/ agent. After organizing the data by date and bank/agent then restructure the transaction of the customer and check the customer details from watch list database. Lastly update AML customers' history database.

Algorithm 4.4: Cash Activity Report Data organizing algorithm

```
1. Input
        Date
        Bank/Agent
2. Filter(date, bank/agent) ⟶ datatable
    //call the data  table  and filter it
3. Set Variables
        Set outputData list is null
        //create empty list for the output data
        Set segregateData list is null
        //create empty list for the segregate data
        Set checkData list is null
        //create empty list for the check data
        Set customerDetail list is null
        //create empty list for customer detail
        Set datedatacontext is null
        //create empty data context for the date data
        Set natIDdatacontext is null
        //create empty data context for national ID detail
        Set datedatacontext is null
        //create empty data context for the date data
        Set natIDdatacontext is null
        //create empty data context for national ID detail
        Set bankAgentdatacontext is null
        //create empty data context for national ID detail
 4. outputData ⟵ FilterBy(date, bank/agent)
   //assign the filter data to the out put
```

```
            Set filterDateData is null
            //create empty data context for the date data filter
            Set filterbankAgentData is null
             //create empty data context for bank/agent detail
       Datedatacontext ⟵ datatable
       bankAgentdatacontext ⟵datatable
       If date is valid and bank/agent exists Then
           For every row element of datedatacontextendRow
               For every row element of bankagentdatacontextendRow
                       Return   filterDateData ⟵ datatable
                      Return   filterbankAgentData ⟵datatable
                Next For
              Next For
             End for
           End for
      Else
         Display_Message("Invalid date or
         Bank/Agent does not    exist")
         Return
      End If
5. segregateData ⟵segregateBy(natID,date)
          //assign the segregate data to the out put
6. segregateBy(natID,date) ⟶ datatable
         //call the data table  and segregate it
         Set segregateDateData is null
         //create empty data context for the date data
         Set segregatenatIDData is null
         //create empty data context for national ID detail
         datedatacontext⟵datatable
         natIDdatacontext⟵datatable
         If date is valid and natID exists Then
             For every row element of datedatacontextendRow
                 For every row element of natIDdatacontextendRow
                    Return   segregateDateData ⟵datatable
                      Return    segregatenatIDData⟵datatable
```

```
                Next For
              Next For
             End for
           End for
      Else
         Display_Message("Invalid date or
         national ID does not exist")
         Return
      End If
 7. checkData←──outputData
      //assign the output to the check data
 8. outputData←──CheckWatchlist (natID)
      //check customer from watch list
       While natID do
       //do checking until the end of delinquent list
          If natID exists then
            customerDetail<>←──cusomerBank/Agent,type
            display_message(customerDetail<>)
           Else
            Return  //return the customer not in the list
           End IF
       Repeat
 9. Update(checkData) ←──customerDetail<>
       While checkData do
       //do checking until the end of check data
          If checkData exists then
           Datatable←──customerDetail<>
           Else
           Return  //return the customer not in the list
           End IF
       Repeat
10. Submit (checkData)──→datatable
```

B) CAR Data Analysis Algorithm

Cash Activity Report Analysis algorithm accepts date, bank/agent, amount and frequency to classify the customers by the amount and frequency as the first task and ready each transaction for monitoring. And then filter by date, amount and institutions. Law enforcement bodies request collected manually and check whether there exist matching between the filtered data and collected ones. If there exist case matching then submit the records to the case handling database.

Algorithm 4.5: Cash Activity Report Data analysis algorithm

```
1. Input
        Date
        Bank/Agent
        Amount
        Frequency
2. Select(date, bank/agent) ⟶ datatable
       //select the requested data from the data table
3. Set Variables
   Set selectData list is null
   //create empty list for the selected data
   Set checkData list is null
   //create empty list for check data
   Set customerDetail list is null
   //create empty list to hold customer details
4. selectData ← SelectBy(date, bank/agent)
    //assign the select data to the out put
         Set selectDateData is null
    //create empty data context for the select data
         Set selectbankAgentData is null
    //create empty data context for bank/agent detail
   datedatacontext ←datatable
   bankAgentdatacontext ←datatable
      If date is valid and bank/agent exists Then
      For every row element of datedatacontextendRow
         For every row element of bankagentdatacontextendRow
```

```
                    Return selectDateData ←datatable
                     Return selectbankAgentData ←datatable
                  Next For
                Next For
              End for
          End for
       Else
          Display_Message("Invalid date or Bank/Agent does not
          exist")
          Return
       End If
5. checkData ← compare(selectData,manualData)
    //call compares function
           Selectdatacontext  ← selectData
           Manualdatacontext  ←  manualData
          Do while eachRow in selectdatacontext until endRow
         //repeat for each data
            Do while eachRow in manualdatacontext until endRow
            //repeat for each data
                If match then          //check if match or not
                    checkDatamanual  ←  datacontext
                    //return match data to the list
                Else
                  Repeat
               //repeat until it ends of manualdatacontext
                End IF
           Repeat
         //repeat until it ends of selectdatacontext
      End do
   End do
6. checkData ← Filter(checkData)
   //call filter function
   Set filterData is null
```

```
    //create empty data context for the date data filter
        Checkdatacontext  ← datatable
      If checkData exists Then
          For every row element of checkdatacontextendRow
                 Return   checkData ← datatable
             Next For
          End for
      Else
         Display_Message("Data does not exist")
         Return
      End If
7. CaseMatching(checkData, manualData)
    Do while eachRow until endRow
      //repeat for each data
         If match then
         //check if match or not
         customerDetail<> ←  matchedData<>
              //return match data to the list
         Else
            Repeat     //repeat until it ends
         End IF
   End do
8. Update(checkData) ← customerDetail<>
    While checkData do //do checking until the end of check data
        If checkData exists then
            Datatable  ← customerDetail<>
         Else
            Return  //return the customer not in the list
         End IF
     Repeat
9. Submit (checkData) → datatable
   //submit data to data table
```

C) CAR Case Investigation Algorithm

Cash Activity Report Investigation algorithm accepts data table from case handling database and creates cash activity detective avoidance for the transaction. Once the data context of the data table displayed then case opening, case analysis, case investigation, and case review tasks will be performed within the data displayed. Finally cash activity detective avoidance report will be registered into detective avoidance database.

Algorithm 4.6: Cash Activity Report Case Investigation algorithm

```
1. Input
   manualData
2. DataContext ← manualData
   //compare the data displayed and manual data
3. Set Variables
        Set selectData list is null
        Set caseOpeingData list is null
        Set checkData list is null
        Set caseDetail list is null
        Set DataContext is null //create empty data context
4. selectData ← SelectBy(date, bank/agent)
        //assign the select data to the out put
        Set selectDateData is null
        //create empty data context for the select data
        Set selectbankAgentData is null
        //create empty data context for bank/agent detail
     If date is valid and bank/agent exists Then
         For every row element of datedatacontextendRow
            For every row element of bankagentdatacontextendRow
                 Datedatacontext ← datatable
                 bankAgentdatacontext ← datatable
              Next For
           Next For
        End for
     End for
```

```
      Else
         Display_Message("Invalid date or Bank/Agent does not
         exist")
         Return
      End If
      caseOpeingData ← CaseOpening(selectData)
      //by using the data context case
5. If selectData not opened Then
     caseOpeing → datatable
   Else
     Display_Message("Case already opened!")
     Return
   End If
6. checkData ← Analysis(selectData,manualData)
7. selectData ← CaseInvestigation(checkData)
        While checkData do
         //do checking until the end of check data
              If checkData exists then
                 Datatable ← caseDetail<>
              Else
                 Return  //return the customer not in the list
              End IF
           Repeat
        End do
8. selectData ← CaseReview(selectData)
      While selectData do
   //do checking until the end of selects data
        If selectData exists then
          Datatable ← caseDetail<>  //only viewing the data
        Else
          Return  //return the customer not in the list
        End IF
       Repeat
   End do
```

```
9. selectData ← CaseReview(selectData)
   While selectData do
   //do checking until the end of select data
        If selectData exists then
         Datatable ← caseDetail<>
      //only viewing the data
        Else
          Return  //return the customer not in the list
        End IF
     Repeat
    End do
10.     DetectiveAvoidance(selectData)
        For every row in selectData to endrow
             // search each data to submit
             Submit (selectData<>)  → datatable
             // submit data to data table
               Next row
             //iterate for the next data
        End For
```

4.6.5 Detection Avoidance Report

Detective avoidance report is the final report of money laundering generated from suspicious and cash transaction collected from banks and agents.

The final stage and output for Suspicious Activity Process Model and Cash Activity Process Model is Detection Avoidance Report. At this stage the task is started from getting data from ML surveillance database for suspicious transaction and detective avoidance database for cash transactions and ends up with registering the report as money laundering on watch list database. This activity is performed by FIC Administrator. There are six major tasks to be performed under detection avoidance report. These are Detective Avoidance Report, Suspicious Activity Report, Data Quality Review, Data Qualification Process, Report Dissemination and Register on watch list. The Figure below Figure 4.15 shows that Detection Avoidance and CAR Administration.

- **Detective Avoidance Report**

Detective Avoidance Report is the type of report generated from Detective Avoidance database from cash activity process model.

- **Suspicious Activity Report**

This step of detection avoidance can be performed by generating Suspicious Activity Report from ML Surveillance database. The senior investigator has prepared and submitted ML Surveillance data from this data the administrator generate the report which needs avoidance of the incidence.

- **Data Quality Review**

This review of transaction in relation with clients or customers must have some mandatory fields like customer or clients address, mobile phone, business type, and/or country of remitter. Before going to the next step called report dissemination it is necessary to have the qualified data or full data of transaction or customer/clients.

- **Data Qualification Process**

If the data is not qualified mean is that the data is not complete then it is necessary to have full or qualified data before dissemination of the report. Data qualification process will be supported by the bank branches or agents.

- **Report Dissemination**

Once the data is qualified then report dissemination is next and registers on reporting database. The disseminated report about customer and related transaction mean is that the one which is suspected on money laundering.

- **Register on watch list.**

At the same time of report dissemination there is the task of registering on watch list because the transaction related with customers or clients considered as suspected transactions for money laundering. The suspected transaction, either it is reported in cash transaction or suspected one for money laundering should reside on watch list database.

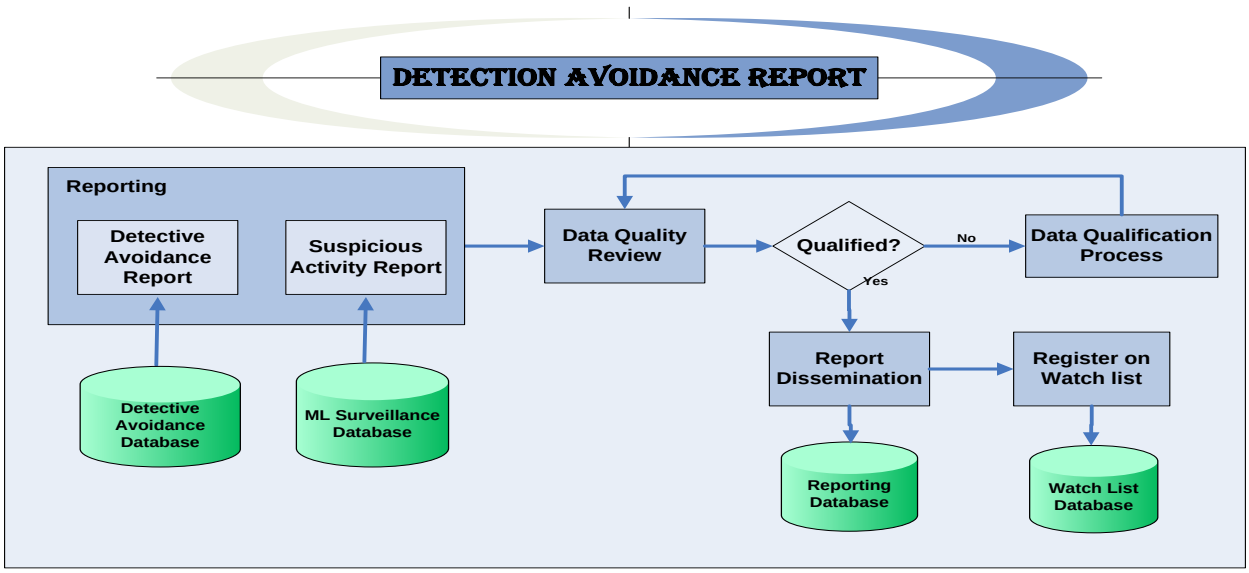


Figure 4.15: Detection Avoidance Report

4.6.6 Detection Avoidance Report Algorithm

Detective avoidance report algorithm accepts the date and bank or agent and returns the data from detective avoidance report for cash transaction and ML surveillance report for suspicious transactions. Under the reporting process there is a task called data quality review and data qualification process. Lastly the algorithm prepares the report to be disseminating responsible organs and update watch list database.

Algorithm 4.7: Detective avoidance report algorithm

```
1. Input
          Date
          Bank/Agent
2. Set Variables
     Set susData<> is null
     //create the list to hold suspicious data
     Set cashData<>is null
     //create the list to hold cash data
     Set dataContext is null    //create the data context
3. Select(date, bank/agent) ⟶ datatable
   //call select function
4. dataContext ⟵ Select(date, bank/agent)
    // function to select data
```

```
          Datedatacontext ← datatable
          Bankagentdatacontext ← datatable
        If date is valid and bank/agent exists Then
         For every row element of datedatacontextendRow
              //search by date
           For every row element of bankagentdatacontextendRow
               If sus then       //suspicious data
                    susDatadate ← datacontext
                    //assign date of suspicious data
                    susDatabank ← agentdatacontext
               Else       //cash data
                    cashDatadate ← datacontext
                    //assign date of cash data
                    cashDatabank ← agentdatacontext
               End if
            Next For
           Next For
         End for
        End for
       Else
          Display_Message("Invalid date or bank/agent does not
          exist")
          Return
       End If

5.dataReview(susData, cashData) → datatable

6. dataReview(susData, cashData)

       IF susData then
        Do while eachRow
          If qulified then
              //check all fields are exist or not (qualification)
              customerDetail<> ← susData
             //assign data to customer list
          Else
```

```
            Dataqualification(susData)
          End IF
         Repeat
       End do
      Else
         Do while eachRow     //do qualification for each column
           If qulified then
             customerDetail<>  ← cashData
           Else
             Dataqualification(cashData)
           End IF
          Repeat   //next for the do while loop until the end
         End do
       End if
7. Dataqualification(anyData)  →  datatable
   //data should be qualified here
8. dataContext  ←  Dataqualification(anyData)
   //return the qualified data
9. Update(dataContext)  ←  dataContext
   //update the customer history
10.     Submit (dataContext) →  datatable
   //submit customer data
```

4.7 Role of NBE in Controlling Money Laundering

NBE is responsible for controlling the banks and financial agents how to process banking activities. There are transactions which needs restructuring and validating the transactions data send to Financial Intelligence Center by banks or agents. All Ethiopian Banks are responsible for transferring cash and suspicious transactional data within the limit to EFIC. In some situations they drop transactions without reporting so that it needs the data validation for the already sent data to FIC. Especially the financial agent's data send to FIC is limited by the amount. The money launderer can perform remittances in different agents and with a multiple incoming messages under the amount limit which affect the country by money laundering. In such cases the National Bank of Ethiopia should monitor and validate the data which is transferred to FIC.

Therefore NBE should have separate systems in order to control money laundering. NBE Remittance Monitoring System and NBE Cash Data Validation System are the two main systems that used to control banks or financial agents with regard to money launderer.

4.7.1 NBE Remittance monitoring system

NBE Remittance Monitoring System is the monitoring of remittance transaction data accessed which is collected from all banks and agents. Figure 4.16 shows the process and workflow of Remittance Monitoring System. These are the major tasks of the system:

- Collect all remittance data from banks and agents.
- Organize the data according to the banks/agents.
- Submit collected and organized data to remittance database.
- Data filtering using the frequency, amount and date interval
- Analyze financial agent's remittances data.
- Restructure the data according to the customer's details and submit to restructure remittance database.
- Generate the restructure report data based on the limit.
- Send the restructure data as special remittance report to FIC for analysis.

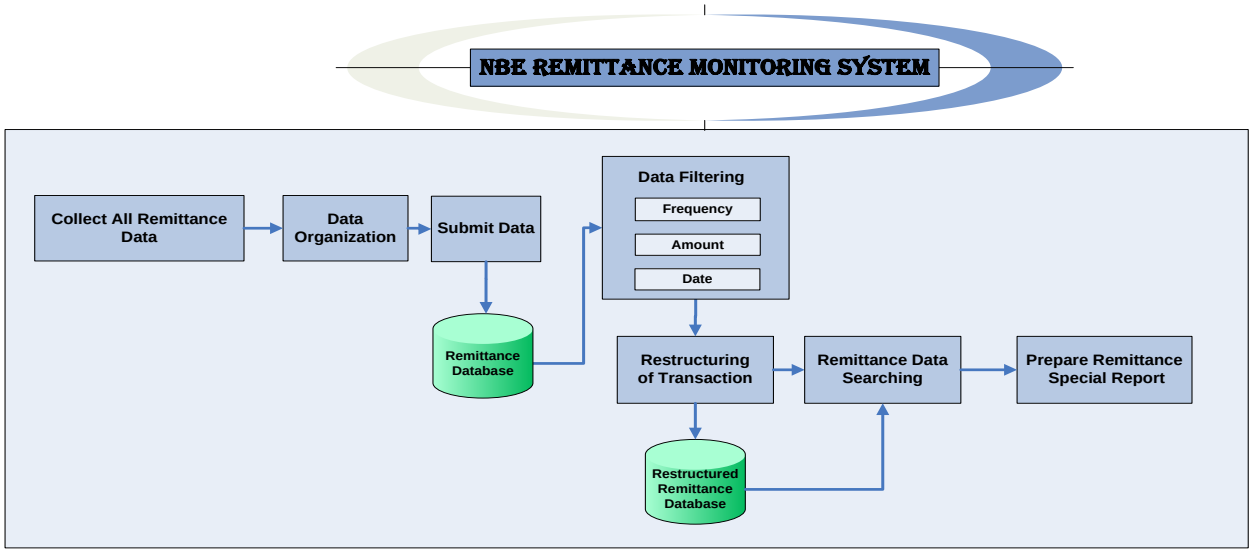


Figure 4.16: Remittance Monitoring System

4.7.2 NBE Remittance monitoring Algorithm

NBE is collecting all remittance data from all financial agents and submitted to FIC database. This algorithm accepts agent name, amount and date of transaction as an input then merge the

transactions to return the transactions sum amount greater or equal to 10,000 USD or equivalent in other currencies. The method of doing such task is called restructuring remittance transaction.

Algorithm 4.8: NBE Remittance Monitoring algorithm

```
1. Input
          Date
          Amount
          Agent
2. Set Variables
     Set remData<> is null
      //create the list to hold remittance data
     Set outputData<> is null    //create the list to hold
     remittance output data
     Set dataContext is null       //create the data context
     Set filterData is null         //create the data context
     Set checkData is null         //create the data context
     Set checkAmount is null
3. Datacontext  ← organizeData(agent)
       //assign the organized data to datacontext
4. submitData(datacontext) → datatable
   // submit the collected data to the data table
5. outputData  ← FilterBy(date, agent)
   //assign the filter data to the out put
6. FilterBy(date, agent)
         Datedatacontext  ← datatable
         Agentdatacontext  ← datatable
         Amountdatacontext  ← datatable
      If date is valid and agent exists Then
          For every row element of agentdatacontextendRow
              For every row element of datedatacontextendRow
```

```
                    Return   filterData ← datatable
                     Return    filterData  ← datatable
                  Next For
                 Next For
               End for
             End for
        Else
           Display_Message("Invalid date or Agent does not exist")
           Return
        End If
7. For every row element of checkDataendRow
            checkAmount ← checkData(amount)
            If    checkAmount greater or equal to 10,000 then
              Return checkData ←  outputdata
            Else
              Return
            End If
              Next For
         End for
8. checkData → datatable
```

4.7.3 NBE Cash Data Validation System

NBE Cash Data Validation System is the managing and validating of cash transaction data accessed from FIC. Figure 4.17 shows the process and workflow of Cash Data Validation System. These are the major tasks of the system:

- Access the FIC Cash Activity Database and Suspicious Activity Database.
- Organize the data according to the banks.
- Submit data to FIC Cash Database.
- Collect banks cash data and submit to Banks Cash database.
- Check and validate using comparison of banks data against to the data sent to FIC using scripts for which resides on databases.
- Identify unmatched data between the FIC and bank data.
- Record the unmatched transactions to the database.

- Report the special cash transactions data which is handled by validation and checking.

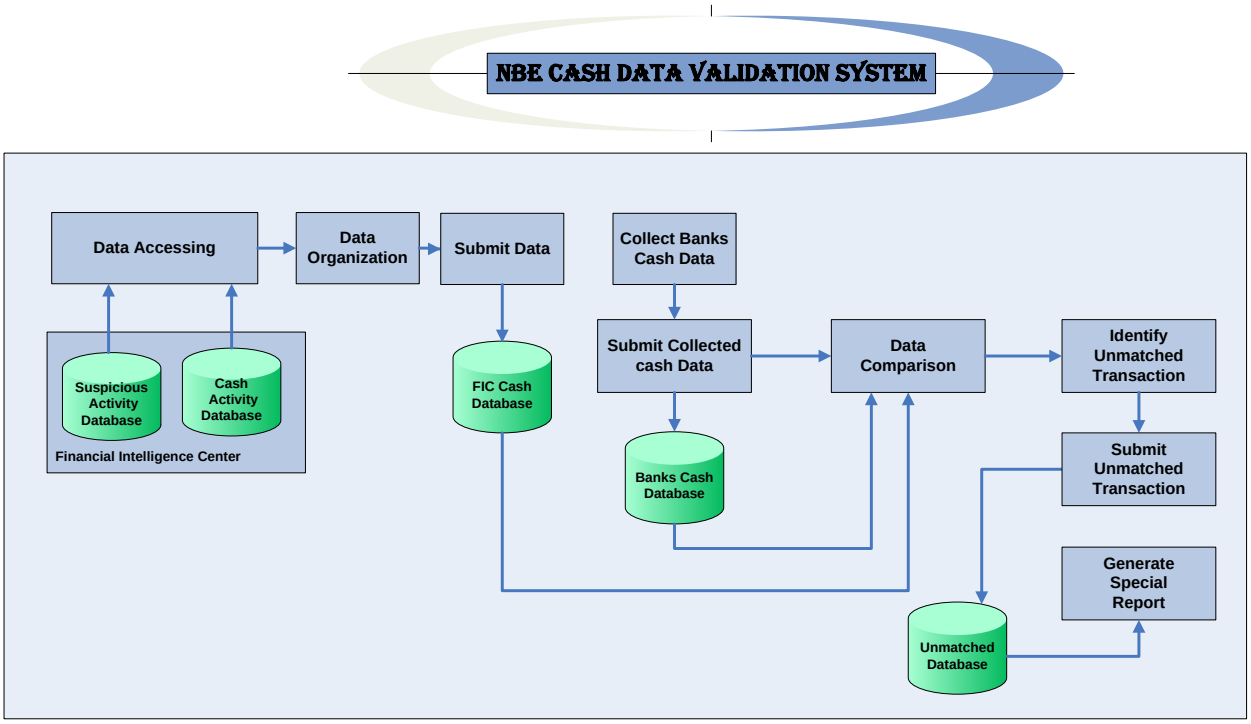


Figure 4.17: Cash Data Validation System

4.7.4 NBE Cash Data Validation Algorithm

As can be seen earlier all banks send their data to EFIC office to which stated amount of cash transaction. Knowingly or unknowingly in some situations the transaction of customers being processed in the banks might not send to EFIC office. One of the responsibilities of NBE is controlling banks transactions and their procedures. Even though this action is illegal it should be controlled by NBE. NBE collects the bank transaction data from their system in order to compare with the submitted data by the banks to EFIC office. This algorithm compares the already collected data against to the submitted data to EFIC office by the banks. And the algorithm accepts two types of data with a number of records, then return the difference between the two. The difference between the two is special type of report used by the FIC office.

Algorithm 4.9: NBE Cash Data Validation algorithm

```
1. Input
        Date
        Bank
2. Set Variables
   Set cashData<> is null
   //create the list to hold cash data
   Set susData<> is null
   //create the list to hold suspicious data
   Set collectcashData<> is null
   //create the list to hold cash data
   Set collectsusData<> is null
   //create the list to hold suspicious data
   Set dataContextone is null
   //create the data context contains collected data
   Set dataContexttwo is null
   //create the data context contains submitted data
3. cashData ← organizeData(date,bank)
4. susData ←  organizeData(date,bank)
5. Submit(cashData) →datatable
6. Submit(susData) →datatable
7. collectcashData ← organizeData(date,bank)
8. collectsusData ← organizeData(date,bank)
9. Submit(collectcashData) → datatable
10.  Submit(collectsusData) → datatable
11.  outputData ← Compare(collectcashData, cashData, date,
   bank)
12.  outputData ←  Compare(collectsusData, susData, date,
   bank)
13.  Compare(DataOne, DataTwo, dateGiven, bankGiven)
       outputData ←  DataOne
       dataContextTwo ←  DataTwo
       Set dataContextThree is null
```

```
For every row element of dataContextOneendRow
  For every row element of dataContextTwoendRow

    If datarow from dataContextone equal to datarow from
    dataContexttwo then
       Return
    Else
      Return datarow  → dataContextThree
    End If
    Next For
  Next For
 End for
15.outputData  →  datatable
```

Chapter Five: Implementation

5.1 Introduction

In this Chapter the prototype implementation of AML software framework for Ethiopian Banks and Financial Agents will be presented as a proof of concept.

In order to test and validate the proposed framework National ID should consider for the implementation. Federal Democratic Republic of Ethiopia Security Immigration and Refugee Affairs Authority have started to implement Ethiopian National ID for an individual. During the start of this research the project of National ID for an individual is under the request for proposal phase. The entire research framework data are based on individual National ID.

Besides the newly developed algorithms for the framework in this prototype, we will discuss the Vince Varallo, a three-layer architecture: the user interface (UI), the business logic layer (BLL), and the data access layer (DAL) [30]. For the purpose of this research the prototype is implemented using Visual Studio 2008 web application and MS SQL 2008 Server Database Management System.

The Chapter is organized into five sections from which the first section provides list of tools and technologies utilized; section 5.2 is about database design, section 5.3 will give framework deployment, section 5.4 will give implementation detail of each layer in the proposed framework and procedure description of major modules there. Prototype demonstration will be described in section 5.5.

5.2 Database Design

For the purpose of implementing the prototype, the logical database design is created. The designed three databases are called FIC Banks/Agents, FIC Activity and FIC NBE. There are tables designed under each database. The database tables are classified into two: setup and transaction tables. The data tables listed below are the standard data format proposed in this research for reporting cash and suspicious transactions data from banks and financial agents to EFIC.

5.2.1 Setup Tables

There are tables which store setup data and useful for both cash and suspicious data handling. These setup tables are Banks, Districts, Regions, Agents, Agent Branches and Bank Branches.

1. **Banks:** This is the table which stores the data of Ethiopian Banks.

2. **Bank Branches:** This is the table which stores the data of Ethiopian Banks with their branches.
3. **Agents:** This is the table which stores the data of Ethiopian financial agents.
4. **Agent Branches:** This is the table which stores the data of Ethiopian agents with their branches.
5. **Regions:** This is the table which stores the data of Ethiopian regions, which is important to find where banks and financial agents are located.
6. **Districts:** This is the table which stores the data of Ethiopia banks districts, which is important to find the banks and financial agents' districts.
7. **Currency:** This is the table which stores the data of all currencies, which is important to identify the transaction.

5.2.2 Transaction Tables

Transactions tables are tables storing transactions data and useful for identifying ML transactions from both cash and suspicious data handled by banks and financial agents. And the data in the database tables are input for cash and suspicious activity process models. In order to classify the data which is collected from banks and financial agents we should consider the data type and source of the data.

- All financial agents' data is remittance in its property. But it can be suspicious or normal remittance data. Therefore we have only two types of data from financial agents.
- The bank data can be cash transaction data or remittance data. Also the remittance data are classified as foreign and local remittance. Therefore here we have three kinds of data but one is the same as the above one which is called foreign remittance data.

In general we have the following data based on the limit of the amount restricted by Ethiopian Proclamation and National Bank of Ethiopia directives in order to show AML software framework for Ethiopian Banks and Financial Agents:

1. Suspicious Agent Foreign Remittance
2. Suspicious Bank Local Remittance
3. Suspicious Bank Cash Transaction
4. Agent Foreign Remittance Report
5. Bank Local Remittance Report
6. Bank Cash Transaction Report

As can be seen above number 1 and 4 are the same in data nature the only difference in between is the data sources, agents and banks. And also number 2 and 5 are the same in data nature except that of the data status one is suspicious and the other is normal local remittance. The same case for cash transactions number 3 and 6 either it can be suspicious or normal cash transaction.

After normalizing each the above transaction tables we have the following tables.

1. **Foreign Remittance:** This is the table which stores the data of all remittance processed through agents. Foreign Remittance is not only from agents but also it is collected from a bank which provides foreign remittance services.
2. **Local Remittance:** This is the table which stores the data of all remittance data processed between banks their branches. This data is collected from banks which give local remittance services throughout the country.
3. **Transactions:** This is the table which stores the data of all cash or suspicious processed by the bank.
4. **Ordering Information:** This table stores the ordering information of the applicant for the foreign remittances.
5. **Account:** This is the table which stores the account information of the cash or suspicious transactions.
6. **Customer:** This is the table which stores the account owner customer information.
7. **Applicant:** This table stores the information about the applicant of the local remittance.
8. **Beneficiary:** This table stores the information of beneficiary in either local or foreign remittances.
9. **Contact Person:** This table stores information about bank or agent branch responsible body or manager of that branch.
10. **Person:** This table stores common information about applicant, beneficiary, customer and contact person.

5.2.3 Proposed framework class diagram

Transactions in the bank is classified by report type, either it can be suspicious or cash. The owner of the account is the bank customer and the legal person who can process the transaction using this account. Local remittance is initiated by the applicant who wants to send the transfer of money and the money is received by the beneficiary of the remittance. Both applicant and beneficiary are the legal persons for that remittance. Foreign remittance holds ordering information from any country to pay it to the beneficiary at the bank branches or agents

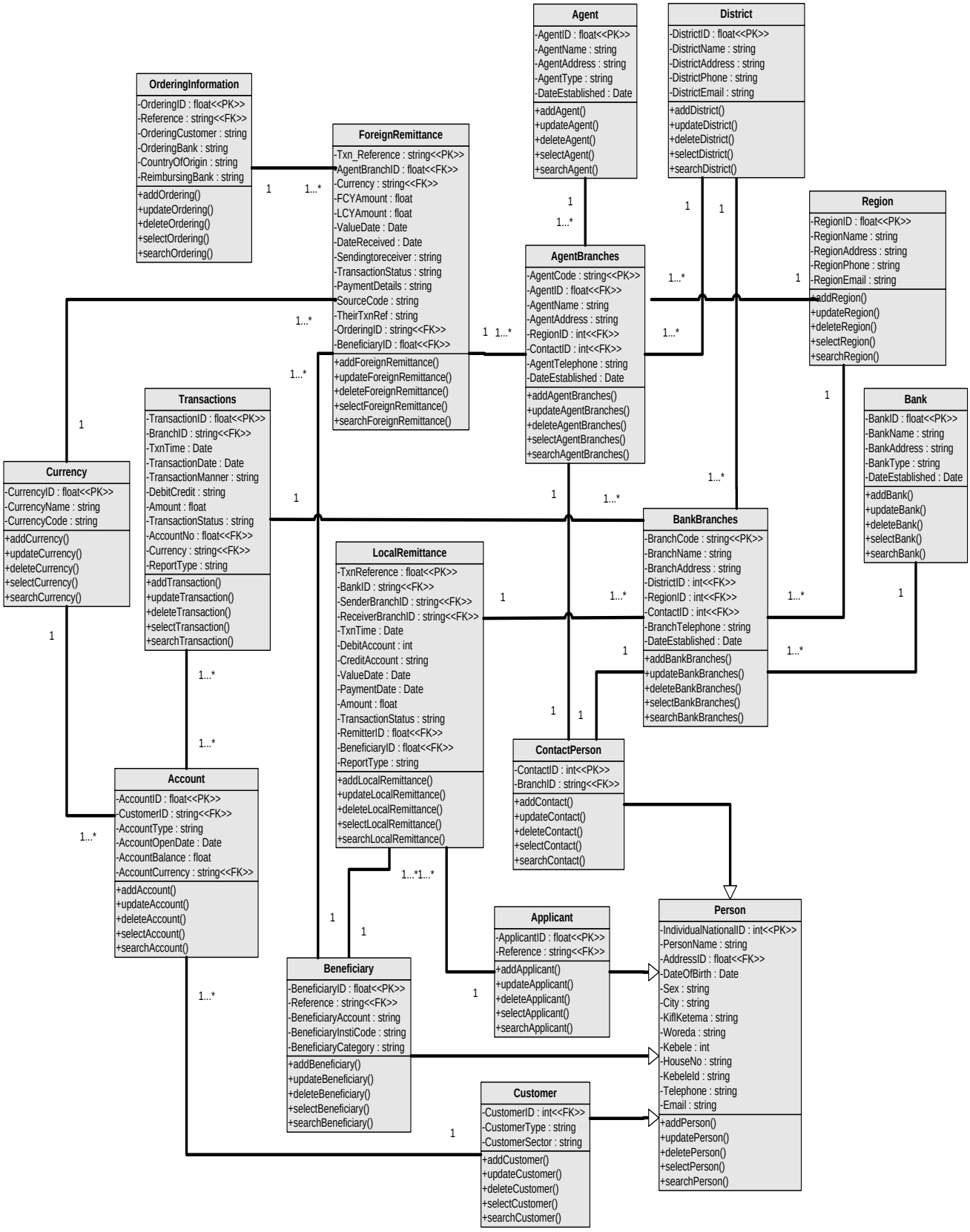


Figure 4.18: Class Diagram for the proposed framework

5.3 Framework Deployment

The proposed framework prototype will be implemented in web based applications which applies client server architecture. Accordingly, the systems and process models are implemented on a web server where the prototype will be developed using ASP.NET with C#. The client computers need only web browsers to request and launch the application from the server. With regards to the data store, the database will be created using MS SQL server. The communication between the client and the server computer will be held via VPN (virtual private network). Figure 5.1 depicts the deployment diagram for the AML Software framework for Ethiopia Banks and Financial Agents.

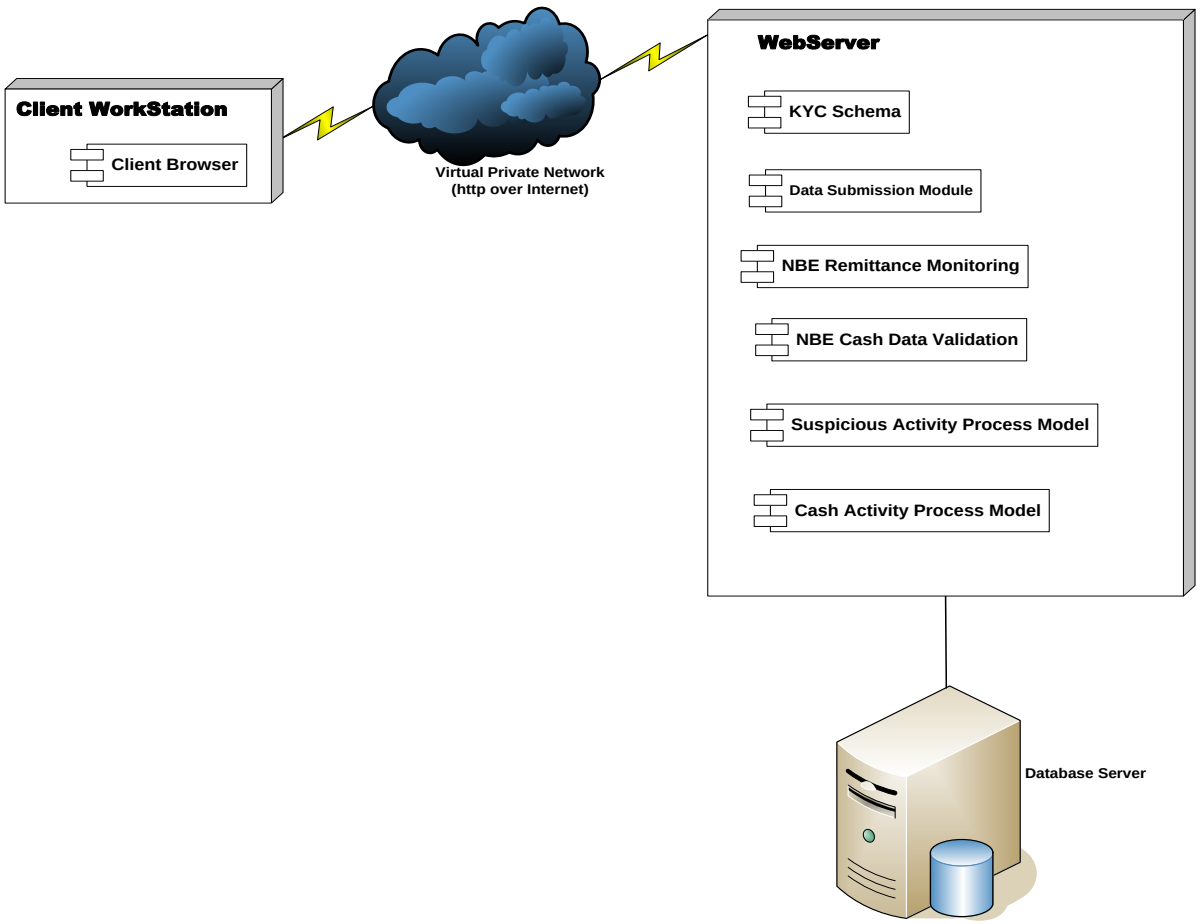


Figure 5.1 : Deployment diagram of AML Software Framework for Ethiopian Banks and Financial Agents

5.4 Implementation Details

In order to visualize the real implementation of the AML software framework in this section we discuss the prototype of the system in detail. The prototype supported by three tier architecture called FIC Data Access Layer, FIC Business Logic Layer and FIC User Interface.

5.4.1 FIC Data Access Layer

The basic task of this layer is presenting the data in standard way to the developer, validating the data and saving the data to the database. The communication between the database and the business logic is managed by FIC data access layer. The FIC data access layer performs CRUD operations against the database. CRUD stands for create, read, update, and delete. To use these features in Visual Studio 2008 it is supported by LINQ to SQL. LINQ to SQL truly helps with rapid application development in communication with database. LINQ stands for Language Integrated Query.

Once the table is added to LINQ to SQL the layer creates override class for delete, insert, select and update statements for the table. In addition to these it creates other utility classes checking duplicate entry and selection from the table by specific field.

5.4.2 FIC Business Logic Layer

The FIC business logic layer primarily contains the main application and interacts with the FIC User Interface and FIC data access layer. According to Vince Varallo Business processes are represented by business entity objects that encapsulate the business rules [30]. The FIC business logic layer removes the complexity of the database from the FIC User Interface that presents data in a more standard way. It also serves to protect the integrity of the data that it passes to the data layer.

Once the data table created in FIC Data Access Layer using LINQ to SQL then the FIC Business Logic Layer is created automatically. The created FIC Business Logic Layer contains two objects called Business Object and Business Object List.

- Business Object

  The business object contains two methods, one for save the record and the other for validation of the records before saves into the database. Both methods are work together during save action called for validation for checking the fields. Here are the steps for creating business objects as shown below.

- Business Object List

This is the method is used for loading search results using one of the field from database table. The algorithm is shown below.

5.4.3 FIC User Interface

This layer contains all user interface classes and modules which are useful for the purpose of displaying data, error messages, common functionality for all pages, enable pages for editing, custom Grid Views for sorting and filtering and classifying the menus according to the purpose and type. These are some of the functionality given by FIC User Interface. Home, KYC, Cash Transaction Data, Suspicious Transaction and Setting Studio and Reports are folders containing user interface modules and pages.

Each folder contains the pages or user interface which can handle the activity as described in its name.

5.5 Prototype Demonstration

Banks and Financial agents can submit their cash and suspicious data using Cash and Suspicious Data Handling System which is the web application developed as a prototype. The first page is login screen shown in Figure 5.2.

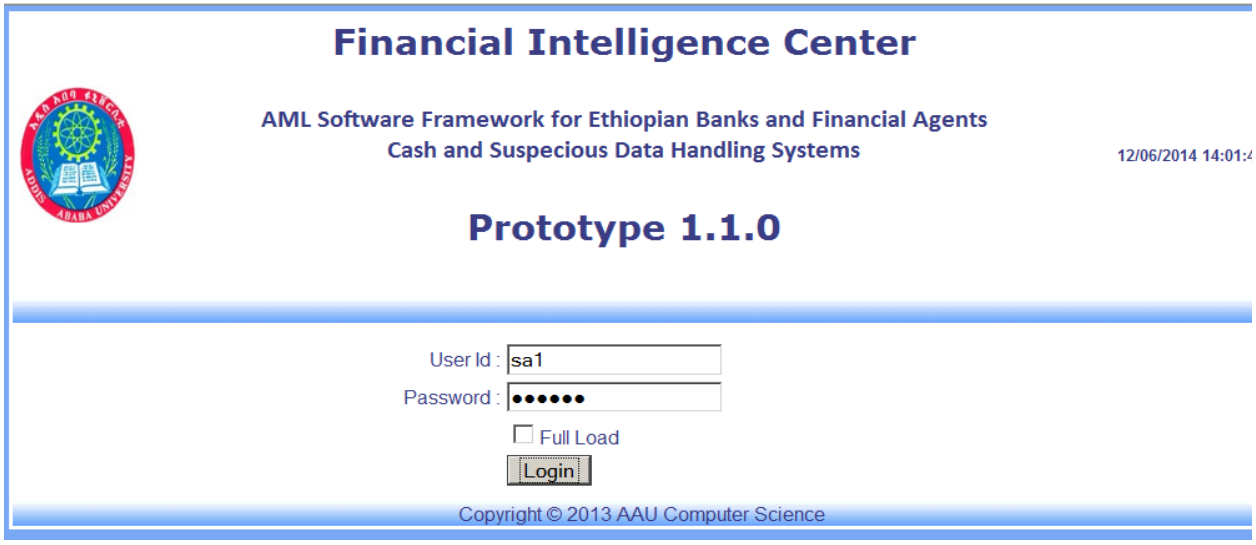


Figure 5.2 : Screenshot for login to the systems

After logging into the system, the system displays the home page containing tabs. Home tab for changing password, Administration tab for user management, KYC tab for applying KYC schema, Cash Handling tab used for handling cash and remittance data of the banks and agents, Suspicious Handling tab applying for submitting suspicious transaction, Setting Studio tab used for registering static information and Reports.

KYC is one of the processes undertaken in opening a bank account which minimizes the risk of banks. Figure 5.3 shows KYC scheme for the client.

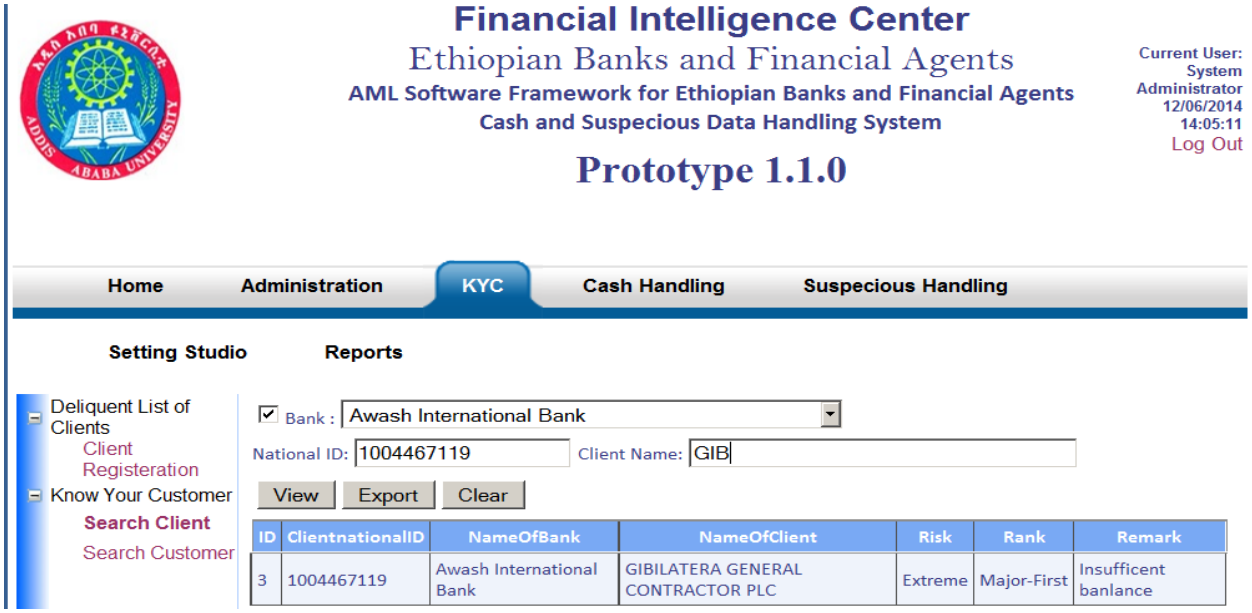


Figure 5.3 : Screenshot for KYC scheme for the client

Cash data handling consists of two types of transactions: cash and remittance transaction. In remittance transaction also there are two categories Agent and Bank remittance. Figure 5.4 shows cash deposit transaction entry.

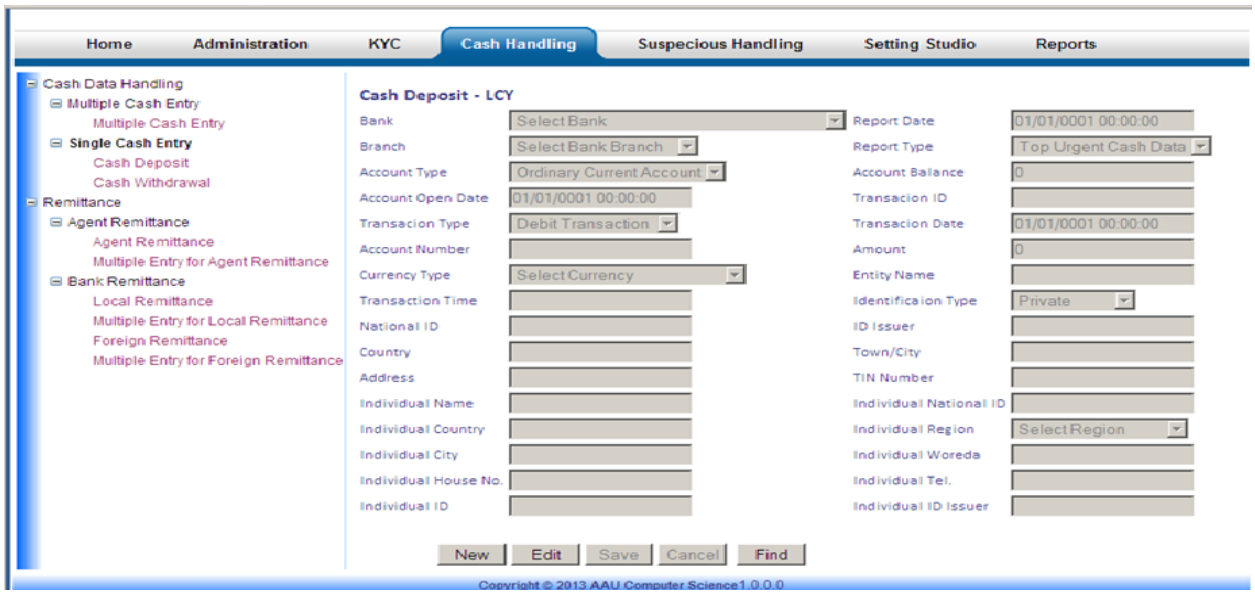


Figure 5.4 : Screenshot for cash deposit transaction entry

Once the data entry is completed we can see the data from data table in the system. Figure 5.5 shows the records submitted to the database.

Figure 5.5 : Screenshot for cash deposit transaction records

Suspicious data handling consists of two processes: agents and banks transaction. Both can be done either in single entry mode or multiple transaction entry modes. Figure 5.6 shows the screen shot for testing multiple entry of suspicious transaction in the prototype.

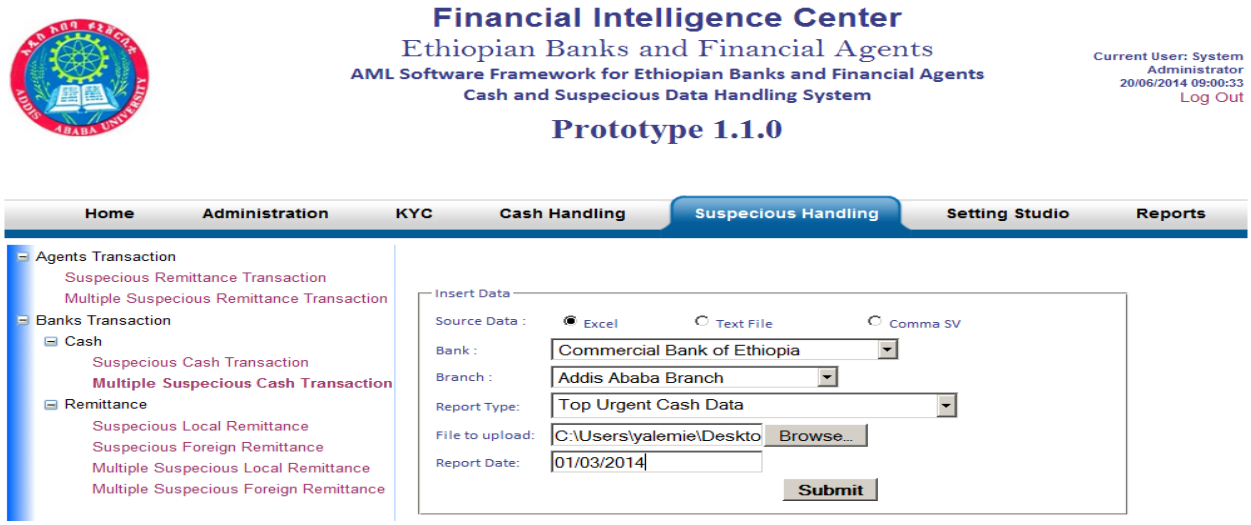


Figure 5.6 : Screenshot for multiple suspicious cash entry

After the data submission by banks and agents the next step will be processing task performed at FIC office. At FIC office two types of tasks will be performed: Cash Activity Report (CAR) and Suspicious Activity Report (SAR) processes. Figure 5.7 shows CAR data organizing in cash activity process model at FIC office.

Figure 5.7 : Screenshot for CAR Data Organizing in Cash Activity Process

The other is suspicious activity process which starts by organizing suspicious data by date range, and by bank or agent. Figure 5.8 shows that data organizing of suspicious transaction.

Figure 5.8 : Screenshot for Data Organizing in Suspicious Activity Process

Chapter Six: Evaluation

This Chapter focuses on the evaluation of our framework, AML Software Framework for Ethiopian Banks and Financial Agents. Evaluation is done by collecting data from banks and financial agents and creating two money laundering cases in order to evaluate the intended output of the framework using the prototype. The first task we performed is data preparation of cash and suspicious transaction data from Banks and eight Financial Agents including giving National ID for each transaction.

The proposed framework mainly used National ID and it is one of the critical aspects to process cash and suspicious transaction. Then here we assume that the National ID is created by randomly generated ten digit numbers that starts with number one in order to avoid data inconsistency. Most of the activities can be performed using the assumption of National ID.

The performance of the framework depends on cash and suspicious data collected from banks and agents, its accuracy using customers National ID, which is uniquely identify the customer. The framework proposed that the data in EFIC office can be available at any time when the request is coming from law enforcement bodies.

To evaluate the proposed framework data was collected from three Ethiopian banks, Commercial Bank of Ethiopia, NIB International Bank, and Bank of Abyssinia. Besides, data from financial agents: TRANS-FAST Remittance, PACO Money Transfer, Kaah Express, World Remitte Ltd., Zenj Exchange, Golden Money Transfer, Dahabshiil, and Blue Nile is collected. Cash and suspicious data are the main sources in evaluating our framework. For this purpose we have collected data from three banks and eight financial agents. The collected data details are shown in Table 6.1 and Table 6.2.

Table 6.1 shows agent remittance data collected from financial agents and banks. The collected data classified by the banks and agents into two: cash and suspicious remittance transactions. As can be seen from the collected data there are banks providing foreign remittance services. For instance at NIB International bank World Remitte Gondar Branch, Jimma Kaah Express and Zenj Exchange Assosa and from Bank of Abyssinya Trans Fast Diredawa and Paco Bahir Dar remittance data collected. The rest of the data collected directly from the financial agents as shown.

Table 6.1 : Agent Remittance Data

Type	Agent Name	Branch	No. of Records	
			Cash Remittance Transactions	Suspicious Remittance Transactions
Agent	Dahabshiil	Addis Ababa Dahabshiil Branch	105	21
	Blue Nile	Blue Nile Mekele Branch	192	58
	Golden Money Transfer	Adama Golden Money Transfer	134	19
Banks	KAAH	Jimma Kaah Express	6	2
	World Remitte	World Remitte Gondar Branch	12	7
	Zenj Exchange	Zenj Exchange Assosa	42	18
	Paco	Paco Bahir Dar	10	3
	Trans Fast	Trans Fast Diredawa	20	6
Total			**521**	**134**

Table 6.2 : Banks and their branch data

No.	Bank Name	Bank Branch Name	No. of Records		No. of Records	
			Cash Data	Suspicious Data	Local Remittance	Suspected Local Remittance
1	**Commercial Bank of Ethiopia**	Addis Ababa Branch	1,194	115	1,490	120
		Mekele Branch	664	62	1,310	65
		Adama Branch	509	42	774	101
2	**NIB International Bank**	Jimma Branch	168	68	908	69
		Gondar Branch	311	45	795	45
		Assoca Branch	120	70	340	91
3	**Bank of Abyssinia**	Bahir Dar Branch	435	43	1,724	120
		Diredawa Branch	278	38	1,007	72
		Hawassa Branch	401	91	1,050	94
Total			**4,080**	**574**	**9,398**	**777**

Table 6.2 shows cash data collected from three commercial banks. The collected data classified into two: cash and suspicious transactions data. Besides it is also as categorized the local remittance as well. During data collection three branches of banks are selected.

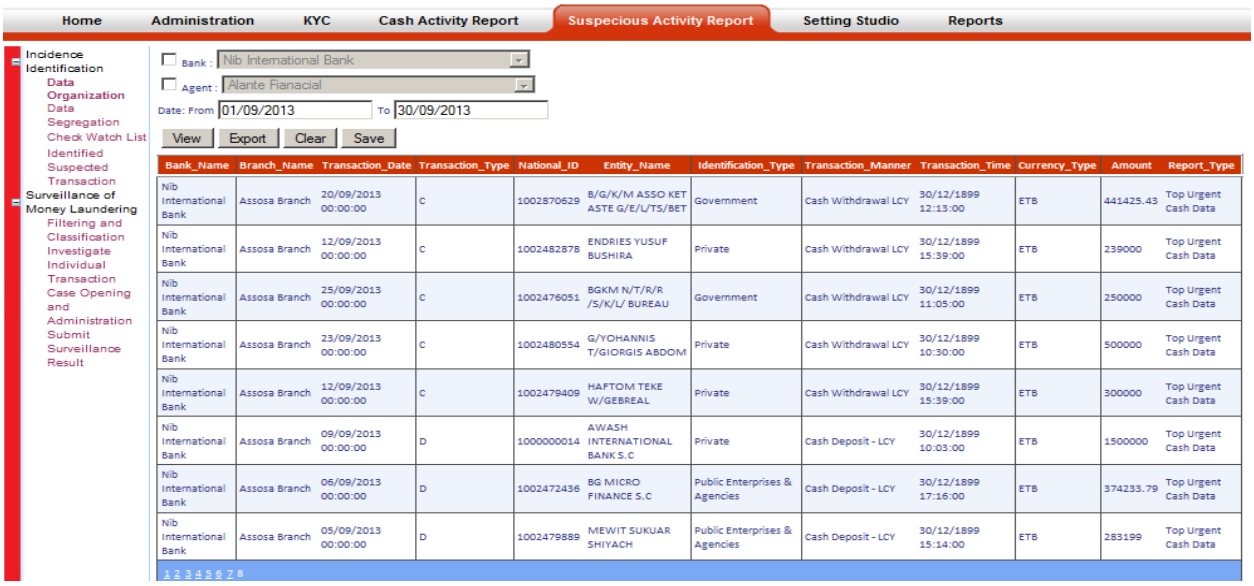
Both Table 6.1 and 6.2 transactions data are input data for evaluating the framework using the developed prototype. These input data are submitted by using data submission module created in the prototype and starts to evaluate the framework works for the intended output or not. The created cases and evaluating the framework demonstrated as follows.

Case I:

Let's assume, an individual involved in illegal activity to get money and deposited that money into one of the banks. An individual tried to conceal the source of fund. The competent authorities need to identify this individual transaction from the banking transactions, who is this individual? Where and when the transaction is processed? What is the amount deposited? Which transaction is suspected from the collected suspicious transactions data? The suspected individual processed banking transactions more than Birr 500,000.00 on September 2013.

In reality this kind of problem exists and necessary to solve it through systematic way. But in the current system to identify this individual is very difficult and time taking. In the proposed framework an individual can easily identify from banks collected suspicious transactions data and report to competent authorities. The steps of identifying the individual from the prototype as follows:

1. Organize the collected data in a given date interval. Figure 6.1 shows the screenshot for suspicious data organizing from 01/09/2013 to 01/09/2013 and save it.

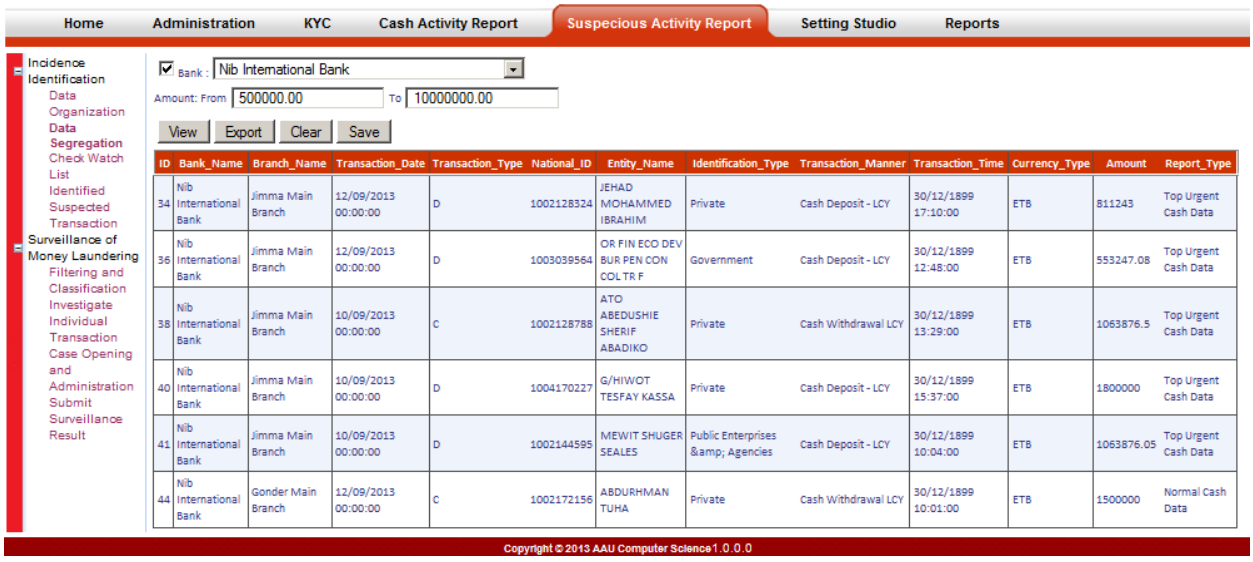


Bank_Name	Branch_Name	Transaction_Date	Transaction_Type	National_ID	Entity_Name	Identification_Type	Transaction_Manner	Transaction_Time	Currency_Type	Amount	Report_Type
Nib International Bank	Assosa Branch	20/09/2013 00:00:00	C	1002870629	B/G/K/M ASSO KET ASTE G/E/L/TS/BET	Government	Cash Withdrawal LCY	30/12/1899 12:13:00	ETB	441425.43	Top Urgent Cash Data
Nib International Bank	Assosa Branch	12/09/2013 00:00:00	C	1002482878	ENDRIES YUSUF BUSHIRA	Private	Cash Withdrawal LCY	30/12/1899 15:39:00	ETB	239000	Top Urgent Cash Data
Nib International Bank	Assosa Branch	25/09/2013 00:00:00	C	1002476051	BGKM N/T/R/R /S/K/L/ BUREAU	Government	Cash Withdrawal LCY	30/12/1899 11:05:00	ETB	250000	Top Urgent Cash Data
Nib International Bank	Assosa Branch	23/09/2013 00:00:00	C	1002480554	G/YOHANNIS T/GIORGIS ABDOM	Private	Cash Withdrawal LCY	30/12/1899 10:30:00	ETB	500000	Top Urgent Cash Data
Nib International Bank	Assosa Branch	12/09/2013 00:00:00	C	1002479409	HAFTOM TEKE W/GEBREAL	Private	Cash Withdrawal LCY	30/12/1899 15:39:00	ETB	300000	Top Urgent Cash Data
Nib International Bank	Assosa Branch	09/09/2013 00:00:00	D	1000000014	AWASH INTERNATIONAL BANK S.C	Private	Cash Deposit - LCY	30/12/1899 10:03:00	ETB	1500000	Top Urgent Cash Data
Nib International Bank	Assosa Branch	06/09/2013 00:00:00	D	1002472436	BG MICRO FINANCE S.C	Public Enterprises & Agencies	Cash Deposit - LCY	30/12/1899 17:16:00	ETB	374233.79	Top Urgent Cash Data
Nib International Bank	Assosa Branch	05/09/2013 00:00:00	D	1002479889	MEWIT SUKUAR SHIYACH	Public Enterprises & Agencies	Cash Deposit - LCY	30/12/1899 15:14:00	ETB	283199	Top Urgent Cash Data

1 2 3 4 5 6 7 8

Figure 6.1 : Screenshot for data organizing by date

2. Data segregation by the amount above Birr 500,000.00 and with in selected bank or all banks. Figure 6.2 screenshot shows for NIB International Bank.



ID	Bank_Name	Branch_Name	Transaction_Date	Transaction_Type	National_ID	Entity_Name	Identification_Type	Transaction_Manner	Transaction_Time	Currency_Type	Amount	Report_Type
34	Nib International Bank	Jimma Main Branch	12/09/2013 00:00:00	D	1002128324	JEHAD MOHAMMED IBRAHIM	Private	Cash Deposit - LCY	30/12/1899 17:10:00	ETB	811243	Top Urgent Cash Data
36	Nib International Bank	Jimma Main Branch	12/09/2013 00:00:00	D	1003039564	OR FIN ECO DEV BUR PEN CON COL TR F	Government	Cash Deposit - LCY	30/12/1899 12:48:00	ETB	553247.08	Top Urgent Cash Data
38	Nib International Bank	Jimma Main Branch	10/09/2013 00:00:00	C	1002128788	ATO ABEDUSHIE SHERIF ABADIKO	Private	Cash Withdrawal LCY	30/12/1899 13:29:00	ETB	1063876.5	Top Urgent Cash Data
40	Nib International Bank	Jimma Main Branch	10/09/2013 00:00:00	D	1004170227	G/HIWOT TESFAY KASSA	Private	Cash Deposit - LCY	30/12/1899 15:37:00	ETB	1800000	Top Urgent Cash Data
41	Nib International Bank	Jimma Main Branch	10/09/2013 00:00:00	D	1002144595	MEWIT SHUGER SEALES	Public Enterprises & Agencies	Cash Deposit - LCY	30/12/1899 10:04:00	ETB	1063876.05	Top Urgent Cash Data
44	Nib International Bank	Gonder Main Branch	12/09/2013 00:00:00	C	1002172156	ABDURHMAN TUHA	Private	Cash Withdrawal LCY	30/12/1899 10:01:00	ETB	1500000	Normal Cash Data

Figure 6.2 : Screenshot for data segregation by amount and bank

3. Check watch list is the process of identifying transactions from segregated data and checking the customer transactions against to the delinquent list. During the check watch list two transactions are displayed and if we select one transactions and click check button to see the transactions details from delinquent list. Figure 6.3 shows the detail of identified transaction.

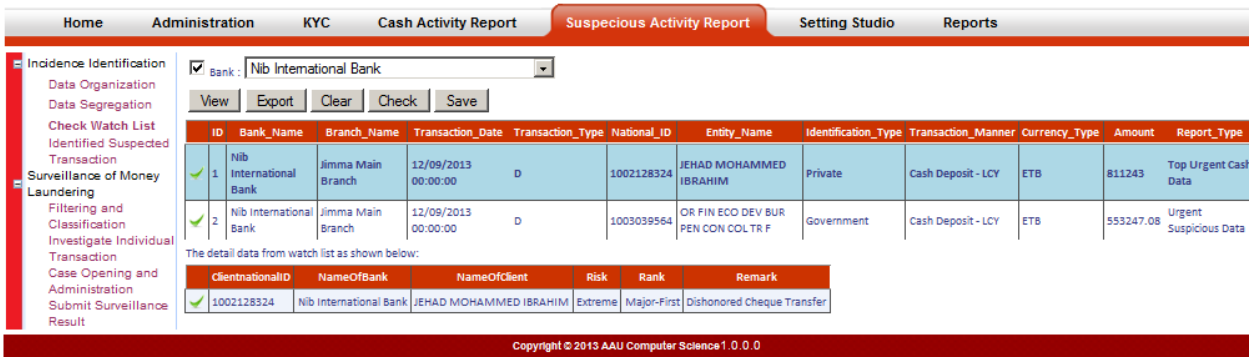


Figure 6.3 : Screenshot for check watch list for the transactions

4. The identified transactions filtered and classified for surveillance of ML. Figure 6.4 shows filtering transactions.

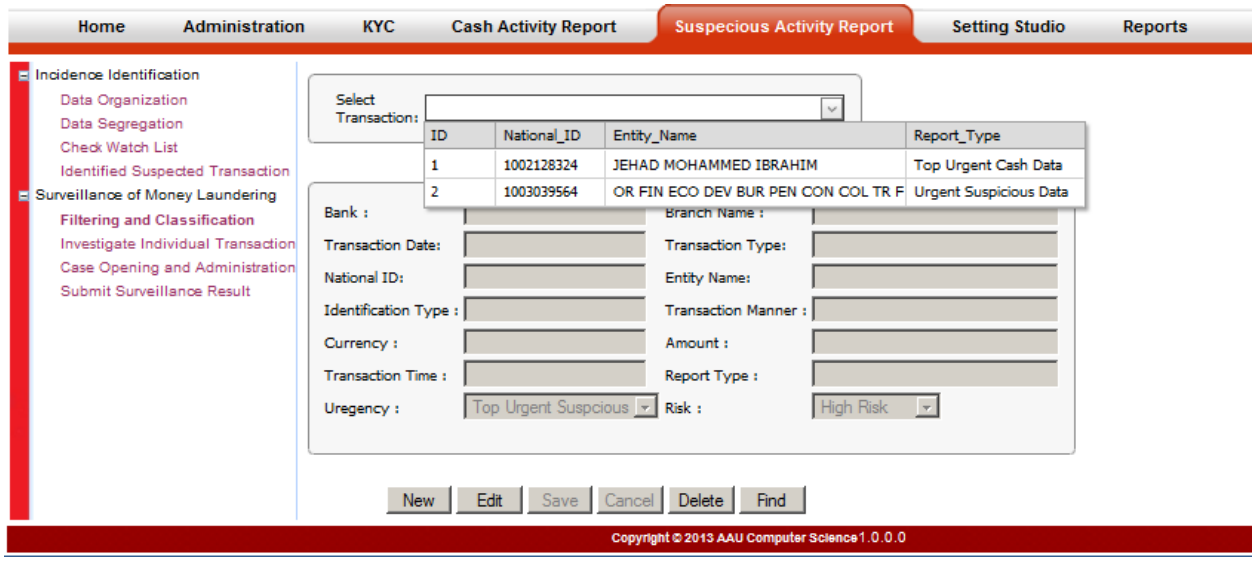


Figure 6.4 : Screenshot for filtering and classification of transactions

5. Investigating individual transaction and case administration, the process of identifying and checking whether the requested transaction exists or not. From Figure 6.5 the first one is government account transaction and the second National Id 1002128324 is a private/ individual transaction.

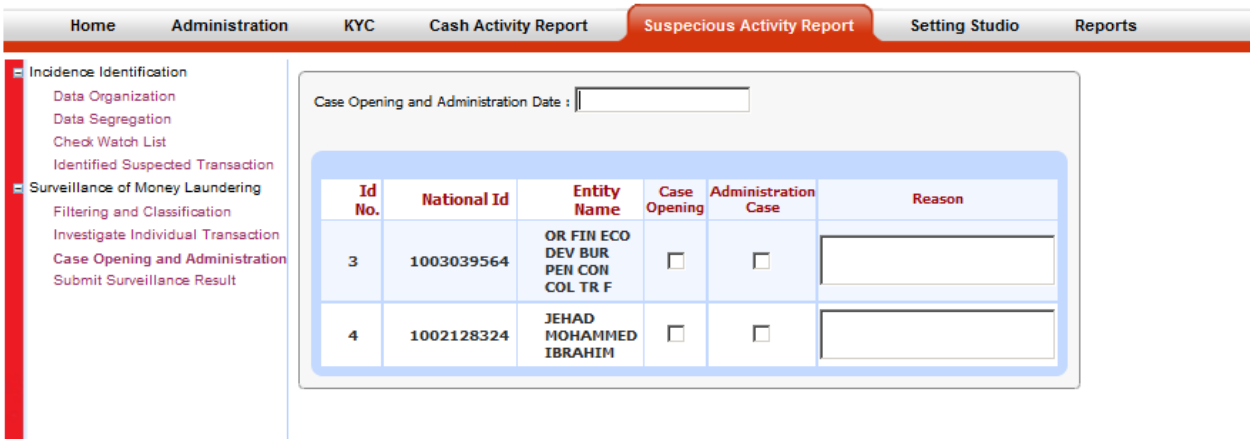


Figure 6.5 : Screenshot for Investigating and case administration transactions

6. Lastly Surveillance result for the requested transaction by competent authorities is shown in Figure 6.6.

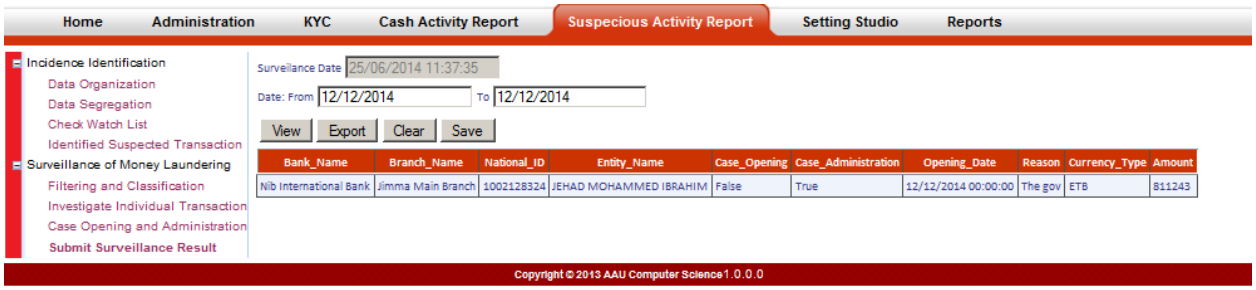


Figure 6.6 : Screenshot for Surveillance result transaction

From surveillance result for suspected transaction is generated from the system in Figure 6.6 we will have the following report:

Bank: NIB International Bank
Date : 12/09/2013
Amount: 811,243.00
Currency: Ethiopia Birr
Customer: JEHAD MOHAMMED IBRAHIM

Case II:

An individual wanted to receive the money in multiple remittances form from different financial agents to conceal the source of fund. The applicant tried to structuring or breaking down the remittances into a number of remittances by the amount less than 10,000.00 USD and sent to the beneficiary. The competent authorities need to identify the beneficiary who receives multiple incoming foreign remittances from abroad with relevant information. Regardless of the financial agents and amounts, the authorities need

the report for June 2013. Who is the beneficiary? How much amount he/she receives? What is the source country for the fund? If possible, who is the ordering applicant for these transactions?

This is a kind of report difficult to generate from one data source in existing system but in proposed framework there is a system called remittance monitoring to handle it. Remittance monitoring is a system supports to collect all financial agents' remittances and submit by data submission module to the system. Once the data submitted then restructure or sum up the amount of remittance based on the beneficiary national ID to report suspected remittance transaction. Therefore the following steps show the collected foreign remittance restructuring for a month of June 2013 from the developed prototype.

1. Figure 6.7 shows the collected and submitted foreign remittance data.

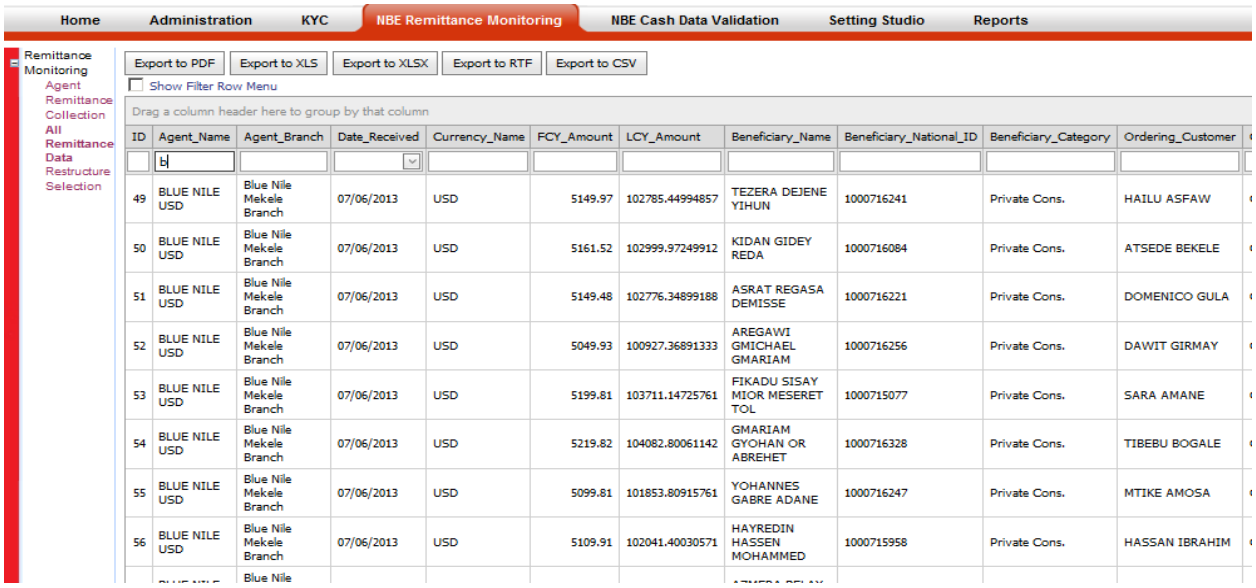
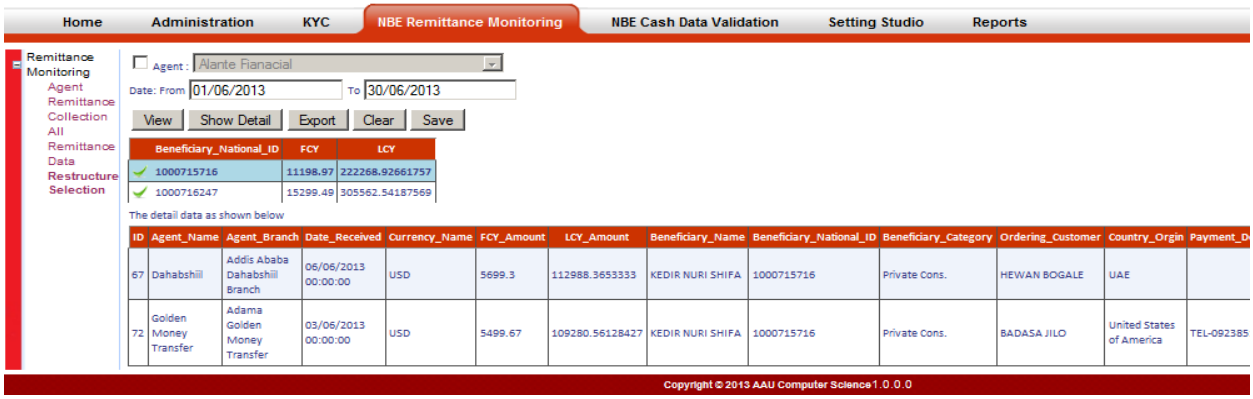


Figure 6.7 : Screenshot for collected foreign remittance data

2. Restructured foreign remittance data based on nation ID as shown in Figure 6.8.



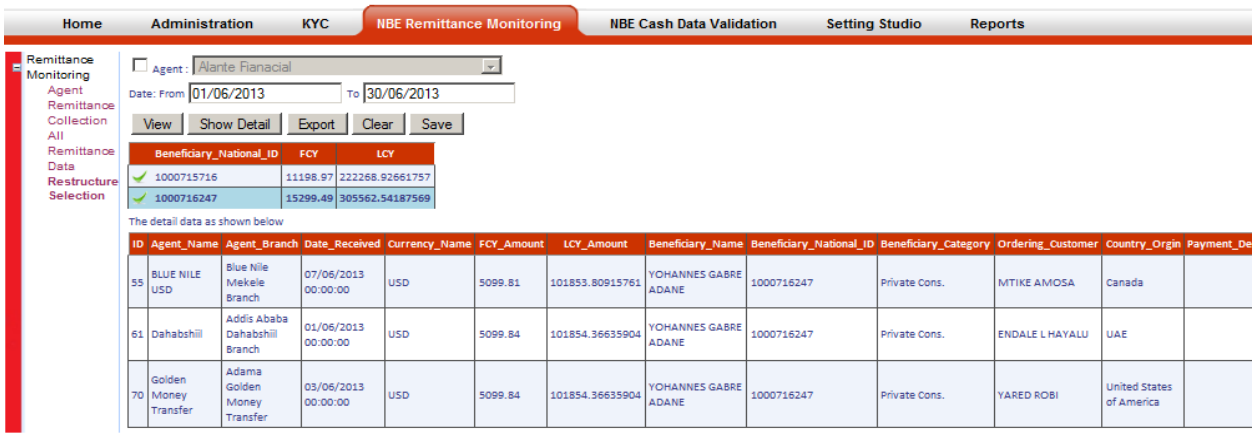


Figure 6.8 : Screenshot restructure foreign remittance data

As can be seen in Figure 6.8 two clients transactions report will be displayed as suspected remittance transactions. The intended financial information for the case reviewed from foreign remittance data as shown in Table 6.3.

Table 6.3: Report for restructure foreign suspected remittance transactions

Beneficiary Name	National ID	Agent	Country of Origin	Amount	Currency	Total Amount	Total Local Amount	Ordering Applicant
KEDIR NURI SHIFA	1000715716	Addis Ababa Dahabshiil Branch	UAE	5,699.3	USD	11,198.97	222,268.92	HEWAN BOGALE
KEDIR NURI SHIFA	1000715716	Adama Golden Money Transfer	USA	5,499.67	USD			BADASA JILO
YOHANNES GABRE ADANE	1000716247	Blue Nile Mekele Branch	Canada	5,099.81	USD	15,299.49	305,562.54	MTIKE AMOSA
YOHANNES GABRE ADANE	1000716247	Addis Ababa Dahabshiil Branch	UAE	5,099.81	USD			ENDALE L HAYALU
YOHANNES GABRE ADANE	1000716247	Adama Golden Money Transfer	USA	5,099.84	USD			YARED ROBI

Chapter Seven: Conclusion and Future Work

7.1 Conclusion

Money Laundering is a sophisticated crime that promotes illegal profit without compromising the criminals who wish to benefit from the proceeds. ML is harm nations and financial systems since illegal money is ultimately integrated with the national economy. Money laundering is the problem to countries in the world, and Ethiopia is also one of a highly risky country in action of ML. But the major problems of ML in Ethiopia is data handling from banks and agents and analyzing and reporting of cash and suspicious transactions from different banks and many financial agents. Also analysis and investigation on SAR and CAR are the major problems as pointed above.

Therefore SAR and CAR must be supported by automation of technological tools in order to generate report for detective avoidance and actions to law enforcement bodies. There are countries which handle SAR and CAR using the automated tools and websites. Besides, banks should have their own Know Your Customer (KYC) policy and identify their own customers. It is also necessary to identify the customer history from the proceeds of National Bank of Ethiopia. AML is difficult task because of the large transactional data, nature of money laundering and heterogeneity of the data. However, the problem can be tackled by solution developers through using clear and easy software framework for AML.

AML software framework which is validated using the prototype of handling and processing of data on cash and suspicious transactions collected from Ethiopian Banks and Financial Agents. And the framework is helpful for the following.

1. EFIC can use the AML software framework for Ethiopian Banks and Financial Agents in order to develop the fully integrated solution to reduce ML attacks.
2. AML software framework helps EFIC for handling of Financial Transactions like data entry, analysis, and reporting.
3. The framework used to improve delivery time of the service for data collection, analysis and reporting from banks and agents to EFIC.
4. The proposed framework supports researchers on AML in Ethiopian Banks and Financial Agents for identifying the problem, in minimizing it and in finding the solutions.

5. The framework enhances monitoring transactions (i.e. Cash and Suspicious) using standardized unique ID for customers of banks and financial agents.

7.2 Future Work

Although the proposed software framework for Ethiopian banks and financial agents is tested and found instrumental in addressing shortcomings of the existing systems, to improve the framework the following key issues need to be addressed.

1. Design integrated framework for Ethiopia Financial Institutions which is fully conversant with different forms used in all banks, financial agents, insurances, micro finances, FIC and competent authorities to handle and process money laundering automatically. This can be automated by registering court cases, customer's history, etc. This system will provide most accurate and complete solution for detecting, investigating and reporting on potential illicit activity.
2. Develop the system performance analytics for EFIC which mitigates risk associated with money laundering. The system includes fully auditable process for the proof of customer due diligence.
3. Develop data mining framework for Ethiopian banks and financial agents which is normally consisting of layers corresponding to levels of mining: transaction, account, institution and multi-institution.
4. Creating artificial intelligence approach for AML for the given transactional data collected from different Ethiopian banks and Financial Agents.
5. Develop multi agent systems supports cash and suspicious data handling and processing which applied for Ethiopian banks and financial agents.

References

[1] http://www.csi.ucd.ie/content/saas-software-service-analysing-financial-datasets-private-cloud-platform-detect-suspicious - Last Accessed on Dec 04, 2012

[2] Money Gram. *Anti Money Laundry Compliance Guide, Latin America and the Caribbean, Report Requirements.* Latin America: Anti Money Laundry Documentations, 2008.

[3] http://www.fatf-gafi.org/topics/high-riskandnon cooperativejurisdictions/documents/cooperativejurisdictions/documents/fatfpublicstatement-24june2011.html – Last Accessed on Dec 02, 2012

[4] Negartet Gazeta - *A Proclamation on the Prevention and Suppression of Money Laundering and Financing of Terrorism* , Proclamation No. 780/2013, February 4, 2013.

[5] http://www.fatf-gafi.org/topics/high-riskandnon- cooperativejurisdictions/documents /fatfpublicstatement-24june2011.html – Last Accessed on Nov 12, 2012

[6] http://en.wikipedia.org/wiki/FATF_blacklist - Last Accessed on Oct 12, 2012

[7] http://www.laundryman.u-net.com/page1_hist.html- Last Accessed on March 11, 2013.

[8] Vijay Kumar Singh. *Controlling Money Laundering in India-Prospects and Challenges*. India; Hidayatullah National Law University, Raipur,January 2009.

[9] John McDowell. *The Consequence of Money Laundering and Financial Crime*, Vol. 6 No.2:USA,Bureau of International Narcotics and Law Enforcement Affairs, An Electronic Journal U.S. Department of State, May 2001.

[10] Şener Daylan(2008), *Combating the Financing of Terrorism: Rethinking Strategies for Success,*Vol. 1, No. 1. DefenseAgainst Terrorism Review, Spring 2008, 137-153.

[11] https://www.unodc.org/unodc/en/money laundering/laundrycycle.html – Last Accessed on Oct 12, 2012.

[12] Brent L. Bartlett.*The negative effects of money laundering on economic development*. The Asian Development Bank, Regional Technical Assistance Project No.5967, December 2002

[13] http://www.fatf-gafi.org/pages/faq/moneylaundering/, How much money is laundered per year? – Last Accessed on March 11, 2013.

[14] Paul Allan Schott. *Reference Guide to Anti Money Laundering and Combating the Financing of Terrorism, 2nd edition*. Washington DC: IMF and the World Bank, 2008.

[15] The Egmont Group Secretariat. *Egmont Group: Information Paper on Financial Intelligence Units and the Egmont Group*. Canada: The Egmont Group, 2012.

[16] http://www.fatf-gafi.org/pdf/40Recs-2003_en.pdf, Rec.26, The Forty Recommendations, - Last Accessed on March 11, 2013.

[17] http://www.fatf-gafi.org/countries/ - Last Accessed on March 11, 2013.

[18] https://www.fic.gov.za/, South Africa FIC Web Site, - Last Accessed on March 14, 2013.

[19] Mutual Evaluation Report, *Anti Money Laundering and Combating of Financing of Terrorism-Republic of Kenya*, ESAMLG September 2011, P.73-100

[20] Biniam Shiferaw *Money Laundering and Countermeasures: A Critical Analysis of Ethiopian Law with Specific Reference to the Banking Sector*. Ethiopia: AAU Law Department, 2011.

[21] http://www.fatf-gafi.org/countries/d-i/ethiopia/documents/fatfpublicstatement-19october2012.html – Last Accessed on March 11, 2013

[22] National Bank of Ethiopia, Customer Due Diligence of Banks Directive No SBB/46/2010

[23] Nhien An Le Khac. An investigation into Data Mining approaches for Anti-Money Laundering, 2009 International Conference on Computer Engineering and Applications,Vol.2. Singapore: IACSIT Press, 2011.

[24] FIC Republic of South Africa.*FIC Annual Report*. South Africa: Financial Intelligence Center, 31 July 2009.

[25] Shijia Gao, Dongming Xu, Huaiqing Wang, and Peter Green. *Knowledge-based anti money laundering: a software agent bank application*, Vol. 13, No. 2. Emerald Group Publishing Limited, Journal of Knowledge Management 2009.

[26] Quratulain Rajput. *Ontology Based Expert-System for Suspicious Transactions Detection*, Vol. 7,No. 1.Canada: Canadian Center of Science and Education, Computer and Information Science, 2014

[27] Edgar Alonso and Lopez-Rojas, *Money Laundering Detection using Synthetic Data*, The 27th annual workshop of the Swedish Artificial Intelligence Society, Linköping University Electronic Press, May 14-15, 2012.

[28] Zengan Gao and Mao Ye. *A framework for data mining- based anti money laundering research*. Journalof Money Laundering Control, 10(2):170{179, 2007.

[29] Nhien-An Le-Khac, Sammer Markos and M-Tahar Kechadi. *A Heuristics Approach for Fast Detecting Suspicious Money Laundering Cases in an Investment Bank*. World Academy of Science, Engineering and Technology 60, 2009.

[30] VinceVarallo. *ASP.NET 3.5 Enterprise Application Development with Visual Studio 2008*.Wiley Publishing, 2009.

[31] National Bank of Ethiopia 2010/2011, Annual Report, VII Investment

Declaration

I, the undersigned, declare that this thesis is my original work and has not been presented for a degree in any other university, and that all source of materials used for the thesis have been duly acknowledged.

Declared by:

Name: Yalemie Temesgen Demeke

Signature: _____

Date: June 27, 2014

Confirmed by Advisor:

Name: Dejene Ejigu (PhD)

Signature: _____

Date: June 27, 2014

Place and date of submission: Addis Ababa, June 2014.