

Bank of South Sudan Anti-Money Laundering Policy Manual



Bank of South Sudan Anti-Money Laundering Policy Manual

December, 2017

Page 1 of 20

TABLE OF CONTENTS

Acronyms

1.0 Bank of South Sudan Anti-Money Laundering Policy Manual -----	1
1.0 Introduction-----	5
2.0 Anti- Money Laundering scope and definition-----	5
3.0 Objective -----	5
4.0 Risks Management Framework -----	6
5.0 Purpose and Overview of the Policy-----	6
6.0 AML/CFT Institutional Policy Framework -----	7
6.1 General Guidelines -----	7
6.2 Co-operation with Competent Authorities -----	7
6.3 Know Your Customer {KYC}/Client (Due Diligence Procedure)-----	7
6.4 Customer Acceptance Policy -----	8
6.5 The requirement to obtain identification evidence -----	7
6.6 The nature and level of the Business to be conducted -----	8
6.7 Risk-based Approach to KYC -----	9
7.0 Identity Verification-----	9
7.1 Definition of Identity -----	9
7.2 Timing of verification of Identity -----	9
7.3 Institutions identity verification-----	10
7.4 Timeframe for obtaining verification requirements -----	11
7.5 Identification procedures and general requirements -----	12
7.6 Higher Risk Accounts -----	12
7.7 Lower Risk Accounts -----	12
8.0 Documentary Evidence of Identity-----	12
9.0 Identification Procedures for Corporate Entities -----	12
9.1 General Principle -----	12
9.2 Identification Requirements -----	13
9.3 Identification Procedure for Foreign Financial Institutions -----	13
10. Correspondent Banking -----	13
11.0 One-off cash Transactions -----	14
12.0 Monitoring, Recognizing and Responding to suspicious Transactions -----	14
12.1 Definition of a suspicious transaction -----	14
12.2 Cash Management -----	14

12.3 Funds/ Wire Transfers-----	14
12.4 Detection of Suspicious Transaction-----	14
13.0 An Audit Function to test the system-----	15
14.0 AML/CFT Record Keeping -----	15
15.0 Employee Education and Training Program -----	15
15.1 Institutional Policy -----	15
15.2 Contents of the training program-----	16
15.3 Training in respect of suspicious transactions -----	16
16.0 Monitoring employee conduct -----	16
17.0 Protection for staff who report violations-----	16
18.0 Administrative sanctions against staff that violate AML regulations-----	17
19.0 Concluding note -----	17

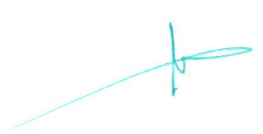
Appendices:

Appendix I

i Money Laundering and Terrorist Financing “Red Flags” -----	19
--	----

Appendix II

ii List of common predicate offences -----	20
--	----



ACRONYMS

AML	Anti-Money Laundering
AMLRO	Anti-Money Laundering Reporting Officer
BSS	Bank of South Sudan
CFT	Combating Financing of Terrorism
CTR	Cash Transaction Report
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FT	Financing of Terrorism
KYC	Know Your Customer
ML	Money Laundering
MLCO	Money Laundering Compliance Officer
PEI	Politically Exposed Institutions
STR	Suspicious Transaction Report

1. Introduction:

The Bank of South Sudan BSS Policy is to comply with all statutes and regulations relating to money laundering and financial crime in general, as well as provide its staff with the correct training to enable them identify suspicious transactions and act in accordance with the regulations so as to protect themselves and the Bank. This trend is further corroborated by the existing legislation on Anti-money laundering and Counter Financing terrorism Act embedded in Anti-money Laundering and Counter Terrorism Financing Act 2012

The Bank of South Sudan views joining the fight against money laundering AML and combating the financing of terrorism CFT as a key priority. BSS is committed to the implementation of all international standards in this area. In order to ensure effective compliance with relevant standards and to preserve South Sudan's reputation as a well-regulated financial Centre, the BSS maintains a Compliance unit tasked with leading the BSS's AML/CFT efforts.

The Compliance Unit is also tasked with handling complaints received from the public relating to Anti-Money Laundering and for receiving information on financial crimes, such as fraud attempts.

2. Anti-money laundering scope and definition

Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in Chapter III of South Sudan Anti-money Laundering and Counter Terrorism Financing Act of 2012.

Terrorism financing is the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist act.

3. Objectives

The Bank has three main objectives when committing itself to the prevention of money laundering:

- i) **Legal and regulatory** – complying with South Sudan Anti-Money laundering and Counter Terrorism Financing Act 2012 and regulatory obligations that impose a series of specific obligations on financial institutions and their employees.
- ii) **Professional** – ensuring that the Bank is not directly or indirectly involved in recycling the proceeds of crime that would call into question its reputation and integrity.
- iii) **Ethical-** genuine cause of taking part in combating crime.

4. Risks Management Framework

Continued watchfulness by the Bank and its staff in the fight against money laundering will protect the Bank from the following risks:

- i) Adverse publicity, loss of public confidence, and loss of business caused by inadvertent association with criminals.
- ii) Regulatory action by the BSS.
- iii) Criminal prosecution and severe penalties in the increasing number of countries in which money laundering is a serious crime.

5. Purpose and Overview of the Policy Manual

This Policy Manual has been formulated by the Bank to reinforce the broad AML/CFT legal requirements and more importantly, to provide best-practice guidance to the Bank's staff on how to implement the relevant legal provisions.

Money laundering (ML) has been defined as the process whereby criminals attempt to or conceal the illegal origin of illegitimate ownership of property and assets that are the fruits or proceeds of their criminal activities. It is, thus, a derivative crime. Financing of Terrorism (FT) is a reverse form of money laundering and may involve both legitimate and illegitimate money. It is characterized by concealment of the origin or intended criminal use of the funds.

Money laundering and terrorist financing are global phenomena and there has been growing recognition in recent times, and indeed, well-documented evidence, that both money laundering and terrorist financing pose major threats to international peace and security and could seriously undermine national development and progress.

Consequently, concerted global efforts have been made to check these crimes. Financial Institutions, in particular, have come under unprecedented regulatory pressure to enhance their monitoring and surveillance systems with a view to preventing, detecting and responding appropriately to money laundering and terrorist financing.

This manual covers the following key areas:

- Design of AML/CFT policy;
- The need to co-operate with the competent authorities ;
- Customer due diligence;
- Monitoring and responding to suspicious transactions;
- Reporting requirements;
- Record keeping;
- AML/CFT employee training program;
- Appendices defining and listing financial and designated non-financial businesses and professions; money laundering "red flags"; and other resource materials.

6. AML/CFT Institutional Policy Framework

6.1 General Guidelines

The Bank of South Sudan is committed to complying with AML/CFT obligations in order to actively prevent any transaction that otherwise facilitates criminal activity or terrorism.

The Bank will, therefore, formulate and implement internal controls and other procedures to deter criminals from using its facilities for money laundering and terrorist financing, thus ensuring that it meets its obligations under the law.

The internal control measures include:

1. Programs to assess the risks related to money laundering and terrorist financing.
2. The formulation of control policy concerned with issues of timing, degree of control, areas to be controlled, responsibilities and follow-ups, to combat money laundering and terrorist financing.
3. Issue circulars, guidelines and enhance the supervisory role on the banking sector.
4. Monitoring programs in relation to unusually large transactions or repetitive transactions; enhanced due diligence with respect to a business's carrying high risks.
5. Enhanced due diligence on corporate institutions in jurisdictions that do not have adequate AML/CFT regimes;
6. Providing employees, including the Compliance Officer, with training on customer due diligence and handling of suspicious transactions, etc.
7. Making the employees to be aware of the provisions of the AML/CFT laws and regulations and the manual of compliance formulated by the Bank, pursuant to those laws.

6.2 Co-operation with Competent Authorities

The Bank will comply promptly with requests, and pursuant to the law, to provide information to the competent authority or other relevant government agency. The Bank's procedures for responding to authorized requests for information on money laundering and terrorist financing shall include:

- a. Immediately searching institutional records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with each individual, entity, or organization named in the request;
- b. Reporting promptly to the requesting authority the outcome of the search
- c. Protecting the security and confidentiality of any such requests.

6.3 Know Your Customer (KYC)/Client (Due Diligence Procedure)

Know Your Customer (KYC) requirement entails obtaining full particulars of the identity of a customer and having adequate knowledge of the purpose for which the customer desires to establish a business relationship with a financial institution. Having adequate knowledge of a

customer and applying it to all transactions initiated by the customer is an effective way of avoiding Financial Institutions being used to launder the proceeds of crime and recognizing suspicious activities.

Thus, the Bank shall establish clear and written procedures for verifying the identity of persons who open new accounts. The procedures should state the types of information the institution will collect from customers and how it will verify each customer's identity.

6.4 Customer Acceptance Policy

The Bank will not establish a business relationship until all relevant counterparties to the relationship have been identified and the nature of the business they intend to conduct has been duly ascertained. Once an on-going business relationship has been established and the normal operation confirmed, any inconsistent activity would be investigated to determine whether there is a suspicion of money laundering.

6.5 The requirement to obtain identification evidence

The first requirement of knowing your customer for money laundering purposes is that the Bank of South Sudan should be satisfied that a prospective customer is the one who he/she claims to be. The Bank of South Sudan shall not carry out, or agree to carry out, any financial business or provide advice to a customer or potential customer, unless the Bank of South Sudan is certain about who that person actually is. If the customer is acting on behalf of another, e.g. the funds are being supplied by someone else, or the investment is to be held in the name of someone else, we have an obligation to verify the Identity of both the customer and the agent/trustee

6.6 The Nature and Level of the Business to be conducted

Bank of South Sudan should obtained adequate information on the nature of the business that the customer intends to undertake, including the expected or predictable pattern of transactions. The information collected at the outset for this purpose should include:

1. Verification of the source of the paid up capital
2. Nature of the activity that is to be undertaken by shareholders and source of their respective funds.
3. Expected origin of the funds to be used during the relationship.
4. Details of other activities and sources of wealth or income

Adequate steps should be taken to keep the information up to date as the opportunities arise, e.g. when an existing customer opens a new account. Such information obtained during any contact with the customer should be recorded and kept in the customer file to ensure, as far as

predictable, that current customer information is readily available to the Compliance Officer or relevant regulatory bodies.

6.7 Risk-based approach to KYC

The Bank shall adopt a risk-based approach in implementing its KYC policy in respect of certain customers who are considered to carry a “higher risk” than others. Generally, the riskiness of customers may depend upon geographical location, customer type, or the product or service being offered to the customers. Such “higher risk” customers who must be subjected to enhance due diligence investigation on risk- based approach include the following:-

- i) Commercial banking
- ii) Correspondent banking;
- iii) Non-face-to-face customers
- iv) Politically exposed institutions.

For such high risk entities, the KYC approach should involve customer risk profiling and assignment of specific risk rates, and the resort to Enhanced Customer Due Diligence techniques (ECDD). The ECDD techniques should include:-

1. Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information (otherwise known as identification data);
2. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the Bank is satisfied that it knows who the beneficial owner is
3. Obtaining information on the purpose and intended nature of the business relationship
4. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Bank knowledge of the customers, their business and risk profile, including where necessary, the source of funds.

7.0 Identity Verification

7.1 Definition;

Identity is defined as a set of attributes, including names used, date of birth, physical features, and the residential address at which a customer may be located, all of which can uniquely identify a natural or legal person. For a natural person, the date of birth should be obtained as an important identifier in support of the name. However, it is not mandatory to verify the date of birth provided by the customer.

7.2 Timing of verification of identity

Identity must be verified whenever a business relationship is to be established and an account opened, or a one-off transaction or series of linked transactions is undertaken. For the purpose of

this manual, the definition of transactions includes the giving of advice. However, advice does not include the provision of information about the availability of products of services or to a first interview/discussion prior to establishing a relationship. Once identification procedures have been satisfactorily completed, and the business relationship established, as long as contract or activity is maintained and records concerning that customer are kept, no further evidence of identity is needed when any transaction or activity is subsequently undertaken.

7.3 Institutions identity verification

a) Customer: Sufficient evidence of the identity must be obtained to ascertain that a customer is who he/she claims to be.

b) A person acting on behalf of others: The obligation is to obtain sufficient evidence of their identities. This requirement is, however, subject to some exceptions, e.g. in consortium lending where the lead Manager/Agent supplies the normal confirmation letter.

c) Furthermore there is no obligation to look beyond the client where:

- i) It is acting on its own account (rather than for a specific client or group of clients);
- ii) The customer is a Bank, broker, fund Manager or other regulated financial institution;
- iii) All the business is to be undertaken in the name of a regulated financial institution.

d) In other circumstances, unless the customer is a regulated financial institution, acting as agent on behalf of one or more underlying customers within the country, and has given written assurance that it has obtained and recorded evidence of identity to the required standards, identification evidence should be verified for:

- 1. The named account holder/person in whose name an investment is registered;
- 2. Any principal beneficial owner of funds being invested who is not the account holder or named investor;
- 3. The principal controller(s) of an account or business relationship (i.e. those who regularly provide instructions); and
- 4. Any intermediate parties (e.g. where an account is managed or owned by an intermediary).
- 5. Appropriate steps should also be taken to identify directors and all signatories to an account.
- 6. Joint applicants/account holders: Identification evidence should be obtained for all the account holders.
- 7. Higher risk businesses undertaken for private companies. Adequate evidence of identity and address should be verified in respect of:
- 8. The principal underlying beneficial owner(s) of the company; and
- 9. Those with principal control over the company's assets (e.g. principal controllers/directors).

10. Officers of the Bank should be alert to circumstances that might indicate any significant changes in the nature of the business or its ownership and make enquiries accordingly.
11. Trusts: Bank Officials should obtain and verify the identity of those providing funds for the trust, i.e. the settler(s) and those who are authorized to invest or transfer funds, or make decisions on behalf of the trust, i.e. the principal trustees and controllers who have power to remove the trustees.

7.4 Timeframe for obtaining verification requirements

The appropriate timeframe for obtaining satisfactory evidence of identity depends on various relevant factors and circumstances, such as the nature of the business, the geographical location of the parties and whether it is possible to verify identify before any commitments could be made or transactions executed.

A Branch staff may start the processing of account opening as soon as a documented request is received, provided that such staff takes diligent steps to verify the customer's identity and does not transfer or pay out funds to a third party until the verification requirements have been duly met.

7.5 Identification procedures and general requirements

- Every official should at all times satisfy itself that he/she is dealing with a real person or organization (natural, corporate or legal), by obtaining adequate identification evidence. Where reliance is being placed on a third party to identify or confirm the identity of an applicant, the overall legal responsibility for obtaining satisfactory identification evidence rests with the account-holding branch.
- The requirement in all cases is to obtain satisfactory evidence that institution of that name lives at the address given and the applicant is that person, or that the company has identifiable owners and that its representatives can be located at the address given.
- Since no single form of identification can be fully guaranteed as genuine or representing correct identity, the identification process should be cumulative.

7.6. Higher Risk Accounts

Higher risk accounts or customers, similar steps should be taken to ascertain the source of wealth/funds.

7.7 Lower Risk Accounts

Even for lower risk accounts or simple investment products, e.g. deposit or savings accounts without cheque book or any of the Bank automated money transmission facilities, there is an overriding requirement for all officers to satisfy themselves on the identity and address of the customer.

8.0 Documentary Evidence of Identity

Care should be taken to ensure that documents submitted are originals in order to avoid the acceptance of forged documents. Copies of documents dated and duly signed, original seen by a senior public servant or a person of comparable status in a reputable private organization may be accepted, pending the submission of the original documents.

9.0 Identification Procedures for Corporate Entities

9.1 General principle

There is particular concern over the ease with which corporate entities could be created and dissolved in some jurisdictions which facilitates the use of these vehicles not only for legitimate purposes but also for criminal activities, such as money laundering. Given the potential risk of misuse of corporate vehicles and the AML protection afforded by factors such as the quality of available information, knowledge of the ultimate beneficial owners as well as the assets and their business objectives, Branch officials should obtain beneficial ownership information and perform customer due diligence at the commencement, and during the course, of a business relationship. This is particularly the case at the account-opening stage.

Furthermore, Branch Management should painstakingly verify the legal existence of the company from official documents or sources and that those persons claiming to act on behalf of the company are duly authorized.

9.2 Identification requirements

The underlying principles of customer identification for natural persons also apply to corporate entities, especially where the identification and verification of natural persons is involved in the relationship with corporate entities.

For agencies, financial institutions and entities, the following information should be obtained:

1. Operational license
2. A letter of introduction from oversea regulators in case of foreign banks attested and verified by foreign embassies
3. Audited financial statements
4. Registered corporate name and any trading names used;
5. Registration or incorporation number in the base country;
6. Principal place of business operations;
7. Mailing address;
8. Contact telephone and fax numbers;
9. Names of Directors and secretary as specified in Form from the base country.
10. The nature of the company's business and its legitimacy; and
11. The resolution of the Board of Directors to open an account and identification of the signatories to the account.

9.3 Identification procedure for foreign financial institutions

Confirmation of existence and regulated status of a foreign financial institution should be carried out by checking with, at least, one of the following sources:

1. The home country Central Bank or relevant supervisory body; or
2. Another office, subsidiary, branch, or correspondent bank in the same country; or
3. A local correspondent bank of the overseas institution; or
4. Evidence of its license or authorization to conduct financial and/or banking business.

10. Correspondent Banking

It is incumbent on the Bank to manage its correspondent banking transactions proactively by taking a risk-based approach. Accordingly, it would have to be ensured that correspondent banks are effectively regulated for Anti-Money laundering control and have effective customer acceptance and KYC policies.

The Bank would not enter into or continue correspondent banking relationships with banks incorporated in jurisdictions which are identified as high risk because they have poor KYC

standards or have been designated as being non-co-operative in the fight against money laundering.

The Bank would guard against receiving funds through its accounts without Treasury or Trade Finance officers taking adequate measures to satisfy themselves that a sufficient due diligence had been undertaken by the remitting bank on the underlying client and the origin of the funds. The Bank would consider terminating its relationship with correspondent Banks that do not respond adequately to customer due diligence and suspicious transactions queries.

11.0 One-Off Cash Transactions

Cash remittances and wire transfers (whether inward or outward) or other monetary instruments that are undertaken against payment in cash for customers who do not have an account or other established relationship with the Bank (i.e. walk-in customers) represent a high risk money laundering category. Thus, adequate procedures should be established to record the transactions and take relevant identification evidence where necessary. Limits for requiring identification evidence should be set at a significantly higher level than that for normal transactions.

12.0 Monitoring, Recognizing & Responding to Suspicious Transactions

12.1 Definition of a Suspicious Transaction

There are numerous types of suspicious transactions, reflecting the various ways in which money launderers operate. For the purpose of this manual, a suspicious transaction may be defined as one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods, such as a transaction that is inconsistent with a customer known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale.

12.2 Cash Management

The Bank shall put in place prudent cash management systems and policies to check "aggregation" of cash deposits and withdrawals made at different times, days, or branches for linked accounts (belonging to the same customer). This shall be done with the aid of an AML monitoring tool.

12.3 Funds/Wire Transfers

Funds transfer requests from customers shall be strictly subjected to AML and Foreign Exchange Acts to guard against any breach. Domestic funds transfers, using the Automated Clearing House and the South Sudan Interbank Settlement Systems shall be effected without recourse to the Treasury Department. Funds transfer outside South Sudan shall be supported with the required documentation before they are effected.

12.4 Detection of Suspicious Transaction

Where a transaction is detected to be suspicious – whether by an internal alert from any of our pay points, or escalated to us by our partners, the bank shall take immediate steps to investigate and where need be, file a suspicious transaction report to the Financial Intelligence Centre and inform our respective partner.

13.0 An Audit Function to Test the System

There shall be an Independent audit function to test the AML system. This periodic audit test will help review the AML/CFT framework with a view to determine its adequacy, effectiveness and completeness.

14.0 AML/CFT Record Keeping

Record keeping is critical to AML/CFT effectiveness. For instance, investigating authorities need to have an adequate audit trail for suspected money laundering transactions and to be able to establish a financial profile of the suspect account. Thus, it is necessary for the Bank to easily access relevant information or documentation at various stages of a transaction.

To accomplish this, document retention policies has been set and procedures would be established for maintaining AML/CFT records. In establishing document retention policy, the Bank would be guided by both statutory requirements and the needs of the investigating authorities on the one hand and commercial considerations, on the other.

The broad categories of AML/CFT-related records are:

- a) Customer identification and verification documents.
- b) Transaction records, including currency transaction reports.
- c) Suspicious transaction reports, together with supporting documentation.

AML/CFT-related records may be maintained by way of original documents, stored in microfiche, and in computerized or electronic form, subject to the provisions of the law on what is acceptable as evidence.

The Compliance Officer or other designated officer shall be responsible for ensuring that all AML/CFT records are maintained properly and kept for not less than six (6) years before they are sent to the archives.

15.0 Employee Education and Training Program

15.1 Institutional Policy

Anti-Money Laundering laws in various jurisdictions impose certain obligations on financial institutions and their staff and prescribe criminal sanctions for non-compliance. It is, therefore, imperative that Head in consultation with the Compliance Officer design comprehensive employee education and training programs not only to make staff fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks.

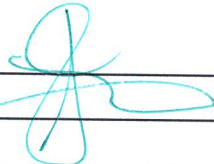
criminal liabilities for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and regardless of whether illegal activity actually happened.

18.0 Administrative sanctions against staff that violate AML regulations

Any member of staff that is suspected or found to have contravened any of the AML regulations like tipping-off, aiding and abetting Money Laundering activities, etc, shall be made to appear before the disciplinary committee of the bank. Such a person when found guilty shall be sanctioned according to the rules of the bank, and may not be insulated from further civil and criminal liabilities under the AML Law.

19.0 Concluding note

In the preparation of this Policy and Manual, deliberate efforts have been made to capture and adopt industry best practice. This document shall be reviewed annually. Nevertheless, should there be a major change in the AML regime whether globally, in the sub region or nationally that calls for adoption, the bank shall co-opt that relevant information into this document.



Othom Rago Ajak
Governor
Bank of South Sudan



APPENDICES

APPENDIX I:

Money Laundering and Terrorist Financing "Red Flag"

1. Introduction

Monitoring and reporting of suspicious transactions is key to AML/CFT effectiveness and compliance. Financial institutions should, therefore, endeavor to put in place effective and efficient transaction monitoring programs to facilitate the process. Although the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of money laundering.

This Appendix, which lists various transactions and activities that indicate potential money laundering, may not be exhaustive but it does reflect the ways in which money launderers have been known to operate.

Since transaction or activities highlighted in this list may not necessarily be indicative of actual money laundering if they are consistent with a customer legitimate business, identification of any of the types of transactions listed here should put financial institutions on enquiry and provoke further investigation to determine their true legal status.

(a) Terrorist Financing "Red Flags"

- 1) Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g. student, unemployed, or self-employed).
- 2) Financial transaction by a non-profit or charitable organization, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organization and other parties in the transaction.
- 3) A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box
- 4) Large number of incoming or outgoing funds transfers takes place through a business account and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high-risk locations.
- 5) The stated occupation of the customer is inconsistent with the type and level of account activity.
- 6) Funds transfer does not include information on the originator, or the person on whose behalf the transaction is conducted, the inclusion of which should ordinarily be expected.
- 7) Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

- 8) Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.
- 9) Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from designated high-risk countries.

APPENDIX II

List of 21 Common Predicate Offences

FATF Designated Categories of Predicate Offences is as Follows:

- i. Participation in an organized criminal group and racketeering.
- ii. Terrorism, including terrorist financing.
- iii. Trafficking in human beings and migrant smuggling.
- iv. Sexual exploitation, including sexual exploitation of children
- v. Illicit trafficking in narcotic drugs and psychotropic substances.
- vi. Illicit arms trafficking.
- vii. Illicit trafficking in stolen and other goods
- viii. Corruption and bribery.
- ix. Fraud.
- x. Counterfeiting currency.
- xi. Counterfeiting and piracy of products
- xii. Environmental crime.
- xiii. Murder, grievous bodily injury.
- xiv. Kidnapping, illegal restraint and hostage-taking.
- xv. Robbery or theft.
- xvi. Smuggling
- xvii. Extortion
- xviii. Forgery
- xix. Piracy
- xx. Insider trading and market manipulation
- xxi. Tax Evasion