SCOPE MARKETS
GLOBAL ONLINE TRADING

Money Laundering and Terrorism (Prevention)
Revised edition 2011

AML POLICY

CONTENTS

Introduction

Scope Market Ltd (hereinafter the "Company") is incorporated under the laws of Belize with Registration number, 145,138 having its registered office at 5 Cork street, Belize City, Belize. Scope Markets Ltd is regulated by the International Financial Services Commission of Belize (IFSC) under license numbers 000274/58 and 000274/57

The Manual is developed and periodically updated by the Compliance Officer based on the general principles set up by the Company's Board of Directors (hereinafter the "Board") in relation to the prevention of Money Laundering and Terrorist Financing.

All amendments and/or changes of the Manual must be approved by the Board.

The Manual shall be communicated by the Compliance Officer to all the employees of the Company that manage, monitor or control in any way the Clients' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

Company's Principles- Legal Framework

As part of our commitment to maintaining the highest ethical standards, and to adhering to all relevant regulations, it is the Company's Manual to prohibit and actively prevent money laundering and terrorist financing. This commitment does not only refer the direct laundering of money, but any activity that facilitates money laundering as well as the funding of terrorist or criminal activities.

Our AML Policy is defined by the MONEY LAUNDERING AND TERRORISM (PREVENTION) ACT CHAPTER 104 REVISED EDITION 2011. This edition contains a consolidation of amendments made to the law by Act No. 18 of 2008.

Money Laundering Definition and Stages of Money Laundering:

Money Laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding criminal prosecution, conviction and confiscation of the illegally obtained funds

The main money laundering stages are:

1. **Placement**: cash are placed into the financial system or retail economy or are smuggled out of the country. The aims of the launderer are to remove the cash from the location of acquisition so as to avoid detection from the authorities and to then transform it into other asset forms for example: travelers' cheques or postal orders

2. **Layering**: is the first attempt at concealment or disguise of the source of the ownership of the funds by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity

3. **Integration**: the money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the "cleaned" money into the economy is accomplished by the launderer making it appear to have been legally earned

Money Laundering Offences:

A person guilty of an offence under the provisions of section 3 of the Act, shall be punishable on conviction:

Natural person, with a fine which shall not be less than fifty thousand dollars, but which may extend to two hundred and fifty thousand dollars, or with imprisonment for a term which shall not be less than five years but which may extend to ten years, or with both such fine and term of imprisonment;

Legal person or other entity, with a fine which shall not be less than one hundred thousand dollars, but which may extend to five hundred thousand dollars.

Organizational Procedures

To ensure compliance with Anti-Money Laundering and Terrorist Financing legislation in force, it is essential to have appropriate and effective organizational procedures in place designed to address the key requirements and facilitate the smooth and at the same time-controlled flow of information and interaction between the various departments.

The Company has herein incorporated the following Customer Identification process as an integral part of the Firm's anti-money laundering compliance program:

a) Customer Due Diligence

The main purpose of the Customer Due Diligence Policy is to protect the Company’s good reputation continuously and consistently, and to prevent the Company from being used for fraudulent or criminal purposes.

The underlying principle of the Customer Due Diligence Policy is that the Company should “know its customers” (Know-your-Client process / “KYC”).

The ultimate responsibility for KYC obligations, both during the process of the establishment and thereafter throughout the life cycle of the relationship, rests with the Compliance function.

The Compliance function is responsible for monitoring developments in the field, identifying required action and informing and training all relevant personnel. The Compliance function is also responsible for the general over-viewing of the application of the prescribed procedures and the improvement / amendment of these procedures if the need arises.

In compliance with the legal framework, the Company applies a risk based approach to Customer Due diligence based on the principles outlined below:

i. Major Determinants of the Due Diligence Process:

- The Company establishes a business relationship;
- In the absence of such a relationship, a Company conducts
  - **a.** any transaction in an amount equal to or above the sum of fifteen thousand dollars (15,000 USD) or such other amount as may from time to time be prescribed by the Minister, whether conducted as a single transaction or several transactions that appear to be linked and where the amount of the transaction is unknown at the time of the transaction, the identification and verification shall be undertaken as soon as the amount becomes known or the said threshold is reached
  - **b.** any wire transfers
- When there is suspicion of money laundering or terrorist financing
- When there is a doubt about the veracity or adequacy of previously obtained customer identification data

ii. Customer Due Diligence Measures:

Such measures comprise of:

- when establishing a business relationship, obtain information on the purpose and nature of the business relationship;

Natural Person:

If the transaction is conducted by a natural person, adequately identify and verify his identity including information relating to

i. the person's name and address;
ii. the national identity card, social security document, passport or other applicable official identifying document;

Specific required documents for a natural person:

As a first step in controlling money laundering, the Company will require all customers to provide valid identification requirements. These documents will then be verified and will undergo thorough screening process.

The Company uses the World-Check database in going beyond knowing the customer using of World check data to screen for heightened risk individuals and entities globally, and to uncover hidden risks in business relationships and human networks.

The customer upon his registration will either be accepted or prohibited to join Scope Markets and its activities; this is upon the discretion of Scope Markets and its employees corresponding to the requirements set out in this policy.

KYC Details - Individual Customer:

1. Customer's full name;

2. Customer's Proof of Identification: Passport Copy or National ID/ Government ID or Driving License
3. Customer's Proof of Address (must be less than 3 months old);
4. Any information prescribed by regulations.

Legal entity:

If the transaction is conducted by a legal entity, adequately identify the beneficial owner of such entity and take reasonable measures to identify and verify its ownership and control structure, including information relating to:

i. the customer's name, legal form, head office address and identities of directors
ii. the principal owners and beneficiaries and control structure;
iii. provisions regulating the power to bind the entity; and to verify that any person purporting to act on behalf of the customer is so authorized, and identify those persons;

Specific required documents for legal entities:

KYC Details - Corporate Customers:

1. Certificate of Incorporation
2. Memorandum and Articles of Association
3. Certificate of Registered address
4. Certificate of Good Standing or Bank Reference letter or Financial Statements of the past year
5. Certificate of Incumbency
6. Certificate of Directors and Secretary
7. Certificate of Shareholders
    a. In case of Nominee(s) in the structure: Trust Deed Agreement
8. For each Authorized Representative, Director, Shareholder (holding 10% or more of the Company Shares) Beneficial Owner:
    a. Passport or ID
    b. Utility bill within the last 3 months
9. If any Shareholder is a legal entity:
    a. Certificate of Incorporation
    b. Memorandum and Articles of Association
    c. Certificate of Registered address
    d. Certificate of Good Standing or Bank Reference letter
    e. Certificate of Incumbency
    f. Certificate of Directors and Secretary
    g. Certificate of Shareholders
10. If any Director is a legal entity
    a. Certificate of Incorporation
    b. Memorandum and Articles of Association
    c. Certificate of Directors and Secretary
11. Operation License (if applicable)

PEPs:

In respect of Politically Exposed Persons (PEPs), at least one of the following measures, or a combination of them, must be applied:

a) The approval of a Director is required for establishing business relationships with PEPs

b) The source of wealth and source of funds that are involved in the business relationship or the transaction must be established

Such accounts are subjected to continuous monitoring.

Shell Banks:

The Company is not opening allowing the establishment of a business relationship with shell banks.

b) AML Risk- Based Assessment

All potential and existing customers are categorized, into three categories: Low / Medium / High Risk. Risks posed by some customers may only become evident only once the customer has commenced trading through his account, making monitoring of customer transactions a fundamental component of the Company's AML Compliance process.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators.

Such indicators include the following:

- the scale and complexity of the services offered
- geographical spread of the services and Clients
- the nature (e.g. non face-to-face) and economic profile of Clients as well as of financial instruments and services offered
- the distribution channels and practices of providing services
- the volume and size of transactions
- the degree of risk associated with each area of services
- the country of origin and destination of Clients' funds
- deviations from the anticipated level of transactions
- the nature of business transactions.

The Compliance Officer shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the Compliance Officer shall also be responsible for the implementation of the policies, procedures and controls on a risk-based approach.

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that must be managed.

The Company shall assess and evaluate the risks it faces, for the use of the its services for the purpose of Money Laundering or Terrorist Financing. The circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the services and the financial instruments that the Company provides are relatively simple, involving relatively few Clients or Clients with similar characteristics, then the Company shall apply such procedures which are able to focus on those Clients who fall outside the 'norm'.

Written Risk Assessment

The AML/CFT risk assessment will be reviewed and updated at least every year at the time of the annual report. This will consider:

- the adequacy, appropriateness and effectiveness of the ratings;
- any significant changes to the composition of Scope Markets' business with respect to the Risk Categories and Types;
- industry guidance and indicators on typologies and emerging trends;
- external opinion / review feedback incorporated; and
- guidance and feedback from the supervisor.

The AML/CFT risk assessment may be reviewed more regularly if there is a material change which could include:

- changes to products and services offered to market;
- changes to the Act, regulations, or guidance which impact on Scope Markets' business operations;
- changes to Scope Markets' AML/CFT programme;
- changes to the nature, size and complexity of Scope Markets's business;
- prior to adopting any new methods of product or service delivery;
- prior to adopting any new or developing technologies used for the provision of a designated service.

Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the Compliance Officer to undertake regular reviews of the characteristics of existing Clients, new Clients, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented, as applicable.

c) Restricted Regions

Scope Markets does not offer its services to the residents of certain jurisdictions such as:

- ⊗ USA
- ⊗ Canada
- ⊗ Japan
- ⊗ Afghanistan
- ⊗ Central African Republic
- ⊗ Congo, Democratic Republic of
- ⊗ Crimea and Sevastopol
- ⊗ Cuba
- ⊗ Eritrea
- ⊗ Guinea
- ⊗ Guinea-Bissau
- ⊗ Iran
- ⊗ Iraq
- ⊗ Korea Democratic People's Republic of (North)
- ⊗ Libya
- ⊗ Myanmar (Burma)
- ⊗ Somalia
- ⊗ Sudan-North
- ⊗ Sudan-South
- ⊗ Syria
- ⊗ Yemen

d) On-going monitoring – Identifying and Reporting Suspicious Activity

Identifying and Reporting Suspicious Activity

Suspicious activity may include identifying patterns of unusual size, volume, or type of transaction, geographic factors such as the choice of banks that are located very far away from the place of incorporation / operations, or any of the «red flags».

The Compliance Officer is responsible for such monitoring, which is done during the normal daily review of trades. Among the information that will be used to determine if an STR should be filed are exception reports that include transaction size, location, type, number, and nature of the activity.

A list of warnings that may signal possible money laundering or terrorist financing ("Red Flags") is attached in Appendix I. The list attached in Appendix I is not exhaustive nor does it include all types of transactions that may be used.
Nevertheless, it can assist the Company and its staff in recognizing the main methods used for money laundering and terrorist financing.

The detection by any member of staff of any of the traits of a "red flag" mentioned in Appendix I prompts further investigation and constitutes a valid cause for seeking additional information as to the source and origin of the funds, the nature and business purpose of the client's transaction, as well as the circumstances surrounding a particular activity performed by the customer. When a member of staff detects any "red flag", he/she will alert the Compliance Officer through an Internal Suspicions Report (Appendix II) who will, in turn, conduct further investigations.

This may include gathering additional information internally or from third-party sources, contacting the relevant government authorities, freezing the account, or filing a STR to the Financial Intelligence Unit (hereinafter as "FIU"). The Compliance Officer receiving the report must remind the person submitting the report about the obligation to avoid the "tipping-off" of the Customer or any other third party and the ramifications of such an act.

The Compliance Officer will issue an Internal Evaluation Report (Appendix III) his / her evaluation and examination of the information received by the Firm's employees and stating the Compliance Officer's final decision on the matter. Irrespective of the outcome of the process, the internal report containing the facts originally submitted and the actions and justification of the decision of the Compliance Officer is archived for future reference.

Notification will not be provided to any person involved in the transaction reported and especially to the suspected customer except as permitted by IFSC regulations.

STR Maintenance and Confidentiality

The Company will keep all STRs and any supporting documentation confidential. It will not inform anyone besides FIU or IFSC. The Compliance Officer will segregate STR filings and copies of supporting documentation from other Company's books and records.

Tipping- off:

It is an offence for a person who knows or suspects that an investigation into money laundering, terrorism or the proceeds of crime has been, is being, or is about to be, conducted, to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

A person guilty of an offence for tipping-off, shall be liable on conviction to a fine not exceeding fifty thousand dollars, or to imprisonment for a term not exceeding three years, or to both such fine and term of imprisonment.

Cash Deposits:

Special attention shall be given from employees in cases the Company receives deposits in excess of $10.000(or its equivalent in any currency.

In such case the Compliance Officer is informed, and the transaction shall be approved by a Director after the completion of enhanced due diligence of the client.

e) Prohibition of third-party transfers

As a general rule, and except from duly justified cases, the Company does not accept any instructions for the transfer of funds or financial instruments to any bank or custody account where the beneficiary is any third party and not the Company's Client.

In duly justified cases, by decision of the Compliance Officer and the Director, the Company might allow 3rd party transfers, upon presentation by the client of authentic documents supporting a valid and legal reason for the transfer.

f) Retention and updating of records

Creation of the Customer Folder / Retention period

The Back Office/Customer Support Department of the Company shall maintain records of:

(a) the Client identification documents and information obtained during the Client identification and due diligence procedures, as applicable
(b) the details of all relevant records with respect to the provision of investment services to Clients

The documents/data mentioned above shall be kept for a period of at least five (5) years, which is calculated after the execution of the transactions or the termination of the Business Relationship.

Updating of records

- Low and Medium Risk accounts: Every year

- High Risk accounts: Twice per year

Duties of the Compliance Officer

Scope Markets must appoint a Compliance Officer who shall be responsible for ensuring the Company's compliance with the requirements of this Act.
Responsibilities of the Compliance Officer:

- establish and maintain internal policies, procedures, controls and systems to
  i. implement the customer identification requirements;
  ii. implement record keeping and retention requirements;
  iii. implement the monitoring requirements;
  iv. implement the reporting requirements this Act;
  v. make its officers and employees aware of the laws relating to combating money laundering and financing of terrorism;

vi. make its officers and employees aware of the procedures and policies adopted by it to deter money laundering and the financing of terrorism; and
vii. screen persons before hiring them as employees;

- establish an audit function to test its anti-money laundering and combating the financing of terrorism procedures and systems; and
- train its officers, employees and agents to recognize suspicious transactions.

Annual Report to the Directors from the Compliance Officer

The Compliance Officer will make a report in writing at least once a year to the board of directors in which he reports on the AML procedures and the suspicions that have been made and acted upon.

Changes may be made or suggested and then implemented on the back of the findings from this report to ensure that the company is always one step ahead of any criminals with regards to AML.

Training Program

The Firm has developed ongoing employee training under the leadership of the Company's Compliance Function.

Training will occur on at least an annual basis or whenever there is a material change in the AML laws and regulations or when the Company's policies and procedures may change. The Compliance Officer will maintain records of the persons who received training, the date of training, the subject matter of the training and a copy of the materials used to conduct the training and a signed list of the people participating will be kept.

Appendix I

Red Flags

The following are a number of warnings that may signal possible money laundering or terrorist financing:

1. The customer or potential customer is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspicious identification or business documents.
2. The customer provides non-verifiable references or is reluctant or refuses to provide financial information or information concerning his/her financial relationships and business activities.
3.The customer repeatedly requests exceptions to policies and procedures set up to deter money-laundering activities (i.e. banking secrecy rules existing in third countries allowing him/her to withhold information).
4.The information provided by the customer that identifies a legitimate source for funds is false, misleading or substantially incorrect.
5. Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
6.The customer (or a person publicly associated with the customer) has a questionable background or is the subject of investigations indicating possible criminal, civil, or regulatory violations
7. The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the Firm's policies relating to the deposit of cash.
8. For no apparent reason, the customer requests multiple accounts under a single name, with a large number of inter-account or third-party transfers.
9. The customer is from a country identified as a non-cooperative country or territory (NCCT) by the FATF.. 10. The customer maintains multiple accounts or maintains accounts in the names of family members or corporate entities, for no apparent purpose.

Appendix II

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name: ..... Tel: .....

Department: .....

Position: .....

CLIENT'S DETAILS

Name: ....

Address: ....

..... Date of Birth: .....

Tel: ..... Occupation: .....

Passport No.: ..... Nationality: .....

ID Card No.: ..... Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction: ....

....

Reason(s) for suspicion:..... .....
....

Informer's Signature Date

....

FOR COMPLIANCE OFFICER USE

Date Received: ..... Time Received: ..... Ref. .....

Reported to the Unit: Yes/No .... Date Reported: ..... Ref .....

Appendix III

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: ..... Client's Details: .....

Informer: ..... Department: .....

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

.....

.....

.....

.....

DECISION

.....

.....

.....

FILE NUMBER .....

COMPLIANCE OFFICER SIGNATURE DATE

.....