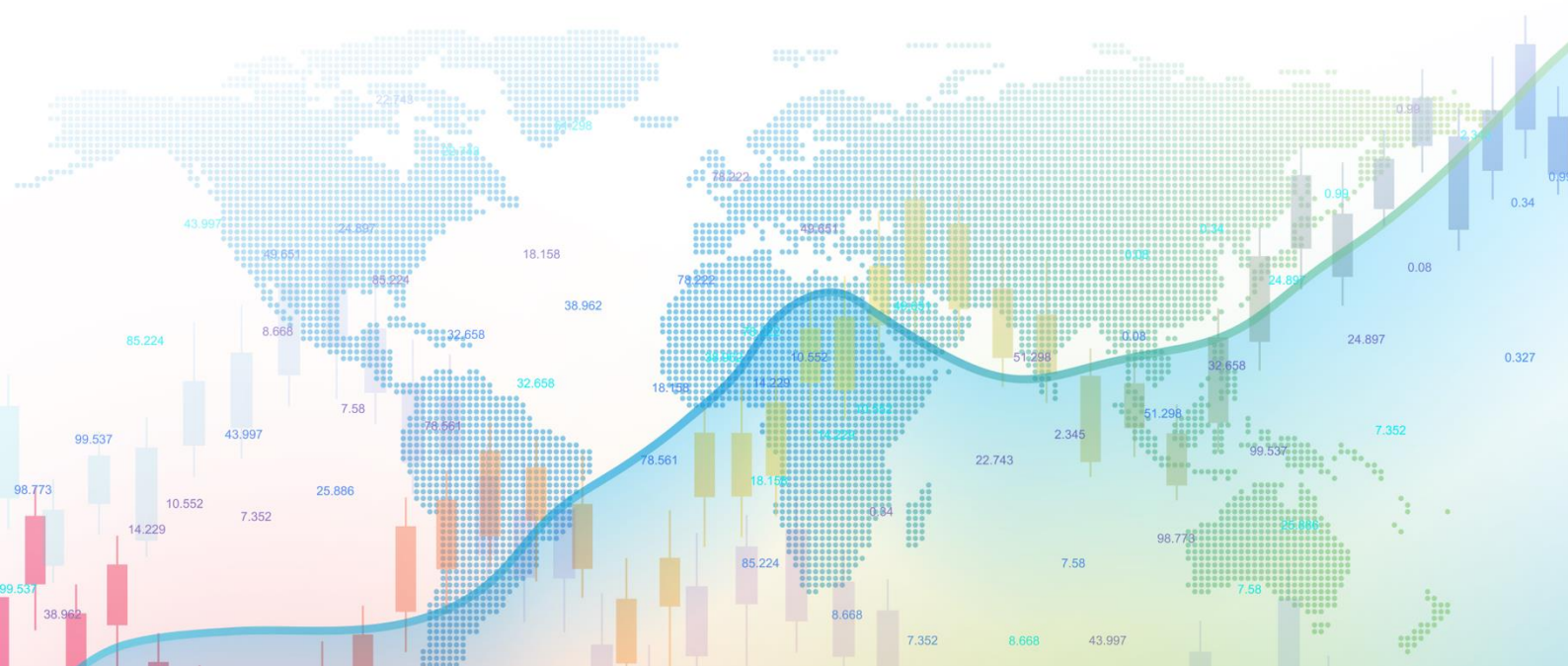


Anti-Money Laundering Policy



Introduction

Scope Markets Global Ltd ("Scope Markets" or the "Company") is a Company incorporated under the Companies Act 1972, with registration number 8426107-1, and registered address Room B11, 1st Floor, Providence Complex, Providence, Mahe, Seychelles.

Scope Markets Global Ltd is a Securities Dealer Licensee, regulated and authorized by the Financial Services Authority (FSA) Seychelles under the license number SD079.

The Policy is provided by the Company to its Clients to assist them understand the procedures followed by the Company to be in compliance with the anti-money laundering and terrorist financing laws and regulations.

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

Legislative Background 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: travellers' 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 is guilty of money laundering if:

- a) he or she directly or indirectly acquires property from the proceeds of criminal conduct;
- b) knowing or believing that property is or represents the benefit of criminal conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse (the proof of which shall lie on the person):
 - i. converts, transfers or handles the property, or removes the property from the

Republic;

- ii. conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights associated with the property; or
- iii. conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights associated with the property; or
- iv. conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights associated with the property; or

Any person who participates in such conduct as described in subsections (1)(i), (1)(ii) or (1)(iii) of this section including but not limited to, aiding, abetting, assisting, attempting, counselling, conspiring, concealing or procuring the commission of such conduct commits the offence of money laundering as a principal offender and shall be liable to be tried and punished as per below:

- a) a person guilty of money laundering is liable on conviction to a fine not exceeding SCR5,000,000 or to imprisonment for a term not exceeding 15 years or to both;
- b) a person other than a natural person guilty of money laundering is liable on conviction to a fine not exceeding SCR10,000,000.

Purpose:

The prevention of money laundering and terrorist financing is of critical importance for the Company's integrity and reputation, and it is the company's main responsibility to identify, report and take measures against money laundering and financing terrorism. For this reason, in order for the Company to prevent the money laundering activities through its services, the following steps are followed:

- Identify and verify the identity of the client by requesting his/her legal documentation.
- Obtain information on the purpose and nature of business relationship.
- Ongoing Monitoring of Clients Activities and Transactions in order to investigate all the suspicious transactions and activities within the Company.
- Identify and report any suspicious activities.
- Maintains all transactions records for at least five years after the termination of the business relationship.

Company Procedures

Client Risk Assessment:

The Company has identified its business-wide risk in which the Company is exposed to Money Laundering/ Terrorist Financing /TF risk (hereinafter referred to as "ML/TF"). The Company has identified and assessed the ML/TF risk in which is associated with the products and services it offers, the jurisdictions it operates in, the customers it attracts and the transaction or delivery channels the Company is using to service its clients.

Identification of Money laundering risks

Risk factors including:

- our clients;
- the products and services we provide;
- the countries that our clients operate in;
- the transactions we are involved in; and
- the delivery channels.

Risk factor 1: Our clients

- The Company identifies the type of clients that its business serves and assesses whether these are known to be frequently used by money launderers.
- The Company separates the clients by industry, size or type (eg, individual, trust, LLP or limited company).

In order to identify all the types of clients that the Company serves, we:

- consider whether any of our principals have industry specialists;
- review our website or promotional material for references to client industry or nature
- consider whether there are certain types of clients that require senior management approval at take-on.

The Company then assesses the risk of money laundering associated with each of those client types. When assessing client risk, we are also considering whether there are any characteristics that are known to be used by money-launderers.

Once the Company has assessed the level of risk associated with each client type, it then identifies any mitigating actions that need to be taken to address this risk. This may include enhanced due diligence, senior management approval at take-on, or updating client due diligence on a very frequent basis.

Risk factor 2: Products and services we provide

- The Company identifies all the services that it offers and assesses whether these could be used by criminals to launder money. In order to identify all the services, we use, the Company takes the following into consideration: the services we are authorised to provide under our license from FSA.

Once the Company has assessed the level of risk associated with each service type, it identifies any mitigating actions that it already has in place or plans to take to address the risk.

Risk factor 3: The countries that our clients reside/operate in

The Company identifies the countries that our clients reside/operate in:

- the countries our clients are based in or operate from;
- where our clients obtain their funding from;

The Company then assesses the risk of money laundering associated with each of those countries. When assessing geographic risk, the Company considers factors such as whether there is a perception of corruption in that country, whether there is known to be criminal activity or if the country is on the sanctions list.

Risk factor 4: The transactions we are involved in

The Company identifies any transactions that it could facilitate and assesses the risk that these transactions could be related to the proceeds of a crime or terrorist financing.

The Company identifies the types of transactions that pass through our clients' money account and assesses the risk associated with each of these types of transaction.

Withdrawals and Deposits processed by the Company's Backoffice Department could also be used to support criminal activity or effect illegal transactions.

The Company then documents its risk assessment of the transactions that it is involved in.

The Company identifies how to mitigate or plans to mitigate those risks. We have set out further guidance on how to address the risks below.

Risk factor 5: Delivery channels

The Company identifies all the methods of interaction it has with its clients. Some delivery channels can increase risk because they can make it more difficult to determine the identity of a client.

Factors to consider are:

- whether we meet our clients face-to-face;
- whether our clients are introduced through an intermediary and whether the Company only corresponds with that intermediary;
- the extent to which the Company relies on the Client Due Diligence (hereinafter referred to as "CDD") of the referrer or intermediary (and the procedures we employ to justify reliance) or the quality of evidence obtained from them to support our own CDD.

Identification Procedures:

According to the AML/CFT Act 2020, the Company is under an obligation to confirm and verify the identity of each customer when establishing a business relationship with the Company. Hence, the following KYC (Know your customer) Documents are request for each of the below categories of clients:

For Individual Clients:

The following types of identity verification are acceptable:

- Current valid passport (showing the first page of the local or international passport, where the photo and the signature are clearly visible); or
- Driving licence which bears a photograph; or
- National identity card (showing both front and back pages)

Proof of Identity (POI) core characteristics:

- If the proof of Identity has expired – is not accepted
- Proof of Identity must always bear a client's photo
- Coloured copies, both sides of the Proof of Identity
- All Sides of the Document to be visible (not cropped)

- The Driving License needs to be issued by a Government/ Public Authority
- **Issuance and expiration date must be clear and visible.**

The following types of address verification are acceptable:

- Documents proving current permanent address (such as utility bills, bank statements, etc.) containing the client's full name (name/surname) and place of residence. These documents should not be older than 3 months from the date of filing.

For Legal persons (Entities):

The data and information that are used for the construction of the Client-legal identification and due diligence shall include, the following:

Limited Liability Entity:

- Completed Corporate Application Form duly signed
- Certificate of incorporation or equivalent.
- Certificate of directors and secretary or equivalent please provide us with:
 - ID and address proofs of all the directors
- Certificate of registered address
- Memorandum and Articles of Association or ByLaws or equivalent.
- Certificate of shareholders or equivalent:
 - ***If Shareholder Natural person (who own 10% or more of the Company) please provide us with:***
- ID and address proofs of all the shareholders (who own 10% or more of the company)
 - ***If Shareholder Corporate person (who own 10% or more of the Company) please provide us with:***
 - i. Certificate of Incorporation
 - ii. Certificate of Directors please provide us with:
 - ***ID and address proofs of all the directors (for non-executive directors, those documents are not mandatory)***
 - iii. Certificate of Shareholders please provide us with:
 - ***ID and address proofs of all the shareholders (who own 10% or more of the company)***

If the above cannot be provided, then a recent (up to 6 months) Certificate of Incumbency.

- Latest Audited Financial Statements (if any) for the last Year or Management Accounts (if any) or a latest bank statement issued on the name of the Company (up to 6 months)

If the above cannot be provided, please provide us with Certificate of Good Standing (up to 1 Year)

- ID and address proof of each authorised person/representative, who does not hold a position of a director or shareholder of the Company.

Public Entity

The list of the required KYC documents for a public Company are the below:

One of the below documents:

- A copy of the dated page of the website of the relevant stock exchange showing the listing.
- A photocopy of the listing in a reputable daily newspaper
- Information from a reputable electronic verification service provider or online registry

In addition to the above, such a legal entity shall provide the Company with:

- A board resolution/authorised signatory list
- Publicly held Company's Website or Annual Report
- Completed Corporate Application Form duly signed

Trusts:

The data and information that are used for the construction of a trust are the below:

- 1) DUE DILIGENCE FORM FOR TRUSTS
- 2) Trust Deed (The trust deed must include the schedule of assets, how and by whom the trust is governed (trustee, protector provisions etc).
- 3) Certificate of Registration

Documentation for the relevant parties (Trustee, Settlers, Beneficiaries and Protector):

- Copy of Passport or ID
- Utility bill of electricity or water or gas or landline, less than 3 months old
- Reference letter from a Bank or Lawyer or Accountant (for the Settlor)
- Detailed Curriculum Vitae (for the Settlor)

Notes:

This represents the minimum documentation that must be provided. Further documentation must be available upon further request.

Regulated entities:

The Company may establish and maintain Business Relationship with the above-mentioned clients and shall request the following for the identification and verification of persons (Beneficial Owner) and company's corporate documents:

In addition to the regular procedure for the limited liability entities, a regulated Company shall provide a copy of the License or authorisation granted to the said entity from a competent supervisory/regulatory authority of its country of incorporation and operation.

Political Exposed Persons (hereinafter as "PEPs"):

Where the Company knows or has reasonable grounds to believe that a client or a beneficial owner

of a client, residing in or outside Seychelles is or becomes a politically exposed person, the Company shall apply, enhanced due diligence measures and enhanced ongoing monitoring.

PEP means:

- (a) an individual who is or has been, during the preceding three years, entrusted with a prominent public function in —
 - (i) Seychelles; or
 - (ii) any other country; or
 - (iii) an international body or organisation;
- (b) an immediate family member of a person referred to in paragraph (a); or
- (c) a close associate of a person referred to in paragraph (a).

The following are close associates of a politically exposed person:

- (a) any person known to maintain a close business relationship with that person or to be in a position to conduct substantial financial transactions on behalf of the person;
- (b) any person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with that person; and
- (c) any person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of that person.

Procedure when dealing with a Political Exposed Person:

The data and information that are used for the construction of the identification and due diligence of a political exposed person shall include, the following

- Verification documents (*please refer to the Identification Procedures of this Policy, for individuals and legal entities*) At the same time, the Company shall proceed with a person's screening through m-check verification tool, to confirm whether the person is a PEP or not;
- take reasonable measures to establish the person's source of funds
- ensure that the person completes the "PEP declaration Form" of the Company
- obtain the approval of senior management before establishing a business relationship with a Politically Exposed person (PEP) or family member or close associate of the PEP
- Declaration Form for PEP

On-going monitoring of suspicious activity

The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a client's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the Client.

The Company shall ensure that it maintains adequate information and knows enough about its

clients' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

In order to identify suspicious transactions, the Compliance Manager with the assistance of the Compliance team shall perform the following activities:

- Monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
- Monitor on a continuous basis if any Client is engaged in any suspicious transactions containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing.

The Company is obliged to report all suspicious transactions and activities to the relevant Authorities and is prohibited from informing the Client that they have been reported for suspicious account activity. Account misuse may result in criminal prosecution.

Restricted Countries

The Company does not offer its services to the residents of certain jurisdictions. Please refer to our Restricted Countries Policy on our website.

Prohibition of third-party transfers

As a 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 Board of Directors, the Company might allow 3rd party transfers, upon presentation by the client of authentic documents supporting a valid and legal reason for the transfer.

Retention and updating of records

The Company shall maintain records of:

- i All documents in opening the accounts of clients and records of all their transactions, especially customer identification records, shall be maintained and safely stored for seven (7) years from the dates of transactions and from the date on which the business relationship ceases.
- ii With respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved for a period of 30 years in digital form, from the date on which the business relationship ceases.

Test of the AML Policy

An independent qualified internal auditor will arrange an annual independent audit regarding the Company's AML policies and procedures, to ensure the Company's compliance with said

procedures. The Company will perform a written follow-up to ensure that any deficiencies noted during this annual review are addressed successfully by the relevant persons.