Rocktrading Ltd

AML & KYC

ANTI-MONEY LAUNDERING – KNOW YOUR CLIENT POLICIES

1. INTRODUCTION

Rocktrading Ltd (the “Company”) aims to actively prohibit, detect and pursue the prevention of money laundering and terrorist financing activities. The Company is also committed to complying fully with all applicable laws, rules and regulations relating thereto, without compromising any of the activities mentioned above.

The Company’s management is committed to compliance with Anti-Money Laundering (“AML”) and Counter-Terrorist Financing (“CFT”) requirements in accordance with applicable laws, and places extremely high importance on the detection and disclosure of any money laundering scheme and/or terrorist financing activities.

Rocktrading Ltd also requires its officers, employees, introducing brokers and affiliated companies to adhere to these standards in order to prevent the use of the Company’s products and services for money laundering and terrorist financing activities.

2. PURPOSE

The purpose of the “AML, CFT and KYC Policy” (the “Policy”) is to provide guidance on the Anti-Money Laundering (“AML”), Counter-Terrorist Financing (“CFT”) and Know Your Customer (“KYC”) measures followed by the Company to achieve full compliance with applicable AML and CTF legislation.

This Policy applies to all Company officers, affiliated companies, and the products and services offered by the Company. Any employee who fails to comply with these policies and procedures will be subject to severe disciplinary action.

3. LEGAL FRAMEWORK

The Company is required to comply with the provisions of applicable laws concerning the prevention of Money Laundering and Terrorist Financing. The primary objective of these laws is to define and criminalize the laundering of proceeds generated from all serious crimes, with the aim of depriving criminals of the proceeds of their crimes.

In accordance with AML and CTF laws, the Company is required to establish policies and procedures to prevent money laundering and terrorist financing activities.

4. DEFINITIONS

4.1 – Money Laundering

Money laundering is the process of creating the appearance that large amounts of money obtained from serious crimes, such as drug trafficking or terrorist activity, originated from a legitimate source.

There are three stages involved in the money laundering process: placement, layering and integration.

4.1.1 – Placement

Placement refers to the act of introducing "dirty money" (money obtained through illegitimate and criminal means).

4.1.2 – Layering

Layering is the act of concealing the source of such money through a series of complex transactions and accounting maneuvers.

4.1.3 – Integration

Integration refers to the act of acquiring or returning such money through apparently legitimate means.

4.2 – Terrorist Financing

Terrorist financing is the process through which funds are provided to finance or financially support individual terrorists or terrorist groups.

A terrorist or terrorist group is one whose purpose or activity is to facilitate or carry out any terrorist action and may involve individuals or groups.

4.3 – AML / CTF

The term AML/CTF refers to "Anti-Money Laundering and Counter-Terrorist Financing" or "Anti-Money Laundering and Countering the Financing of Terrorism".

4.3.1 – Anti-Money Laundering

Anti-Money Laundering ("AML") refers to a set of procedures, laws or regulations designed to prevent the practice of generating income through illegal actions.

4.3.2 – Counter-Terrorist Financing

Counter-Terrorist Financing ("CTF") refers to a set of procedures, laws or regulations designed to prevent the financing of or provision of financial support to individual terrorists or terrorist groups.

4.4 – Financial Action Task Force (FATF)

The Financial Action Task Force on Money Laundering ("FATF"), also known by its French name, Groupe d'action financière (GAFI), is an intergovernmental organization established in July 1989 by the Group of Seven (G-7) summit in Paris, initially to examine and develop measures to combat money laundering.

In October 2001, FATF expanded its mandate to incorporate efforts to combat terrorist financing in addition to money laundering.

The objectives of FATF are to establish standards and promote the effective implementation of legal, regulatory and operational measures to combat money laundering, terrorist financing and other related threats to the integrity of the international financial system.

Beginning with its own members, FATF monitors countries' progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and countermeasures; and promotes the adoption and implementation of the FATF Recommendations worldwide.

The Working Group was responsible for examining money laundering techniques and trends, reviewing actions already taken at national or international level, and establishing the measures that still needed to be taken to combat money laundering.

In April 1990, less than one year after its creation, FATF issued a report containing a set of Forty Recommendations, intended to provide a comprehensive action plan necessary to combat money laundering.

In 2001, the development of standards to combat terrorist financing was added to FATF's mission.

In October 2004, FATF published Nine Special Recommendations, further strengthening the agreed international standards for combating money laundering and terrorist financing: the 40 + 9 Recommendations.

In February 2012, FATF completed a comprehensive review of its standards and published the revised FATF Recommendations. This review was intended to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime.

These standards were expanded to address new threats, such as the financing of the proliferation of weapons of mass destruction. The new standards also impose higher levels of transparency and stricter regulations to prevent corruption.

The nine Special Recommendations on terrorist financing have been fully integrated with the anti-money laundering measures. This has resulted in a stronger and clearer set of standards.

5. PROCEDURES

The provisions of the Laws adopted by the Company introduce procedures and processes that ensure compliance with applicable Laws relating to Money Laundering and Terrorist Financing activities.

5.1 – Customer Categorization and Identification Procedures

The Company has adopted all requirements of applicable laws in relation to customer categorization and identification and customer due diligence procedures, as explained below.

5.1.1 – Customer Categorization

Customers are classified according to their risk profile into three main categories:

- a – Low-Risk Customers

The following types of customers are considered lower risk. The Company will collect sufficient information to establish whether the customer qualifies to be classified as a lower-risk customer:

i – Credit or financial institutions located in another country that impose requirements higher than or equivalent to those established by the Company’s regulators.
ii – Listed companies whose securities are admitted to trading on a regulated market in other countries and which are subject to disclosure requirements compatible with Community legislation.

- b – Normal-Risk Customers

All customers who are neither High-Risk nor Low-Risk Customers will be considered Normal-Risk Customers.

- c – High-Risk Customers

Customers meeting the following criteria are classified as high risk:

i – Non-face-to-face customers.
ii – Customer accounts held in the name of a third party.
iii – Accounts of Politically Exposed Persons (“PEPs”).
iv – Betting / online gambling activities.
v – Customers from countries that inadequately apply FATF Recommendations.
vi – Customers whose nature presents a higher risk of money laundering and terrorist financing.
vii – Any other Customer that the Company itself determines should be classified as such.

5.1.2 – Customer Identification (Due Diligence)

- a – Due Diligence Conditions

Customer Identification and Due Diligence procedures apply under the following conditions:

i – Establishment of a business relationship.
ii – There is a suspicion of money laundering or terrorist financing, regardless of the transaction amount.
iii – There are doubts regarding the adequacy of previously obtained customer identification data.
iv – A customer’s failure or refusal, without proper justification, to provide the data and information required to verify their identity and establish their economic profile.

- b – Timing of Due Diligence

i – Customer identification and due diligence must take place before establishing a business relationship or carrying out a transaction.
ii – Verification of the customer’s identity may be completed during the establishment of a business relationship if necessary to avoid interrupting the normal course of business and where there is a limited risk of money laundering or terrorist financing. In such circumstances, these procedures must be completed as soon as possible.
iii – Reviews of existing records must be performed regularly, ensuring that documents, data or information retained are kept up to date.

iv – A customer's failure or refusal, without proper justification, to provide the data and information required to verify their identity and establish their economic profile.
v – When a customer account is opened, it must be closely monitored.
vi – Customer due diligence procedures will apply not only to all new customers, but also, at appropriate times, to existing customers on a risk-sensitive basis.
vii – At frequent intervals, the Company must compare the estimated account turnover with the actual turnover.
viii – Any significant deviation must be investigated, not only for possible action by the Company in relation to the particular account concerned, but also to assess the reliability of the person or entity that introduced the customer.

- c – Due Diligence Procedures

The practice followed by the Company to comply with legal requirements concerning customer identification is based on a risk-based approach.

i – Standard Customer Due Diligence Procedure
– Identification of the customer and verification of the customer's identity based on information obtained from a reliable and independent source.

– For legal persons, taking appropriate and risk-based measures to understand the customer's ownership and control structure.

– Obtaining information on the purpose and intended nature of the business relationship.

– Continuously monitoring the business relationship, including scrutiny of transactions carried out throughout the relationship, to ensure that the transactions conducted are consistent with the data and information held by the Company in relation to the customer.

ii – Simplified Due Diligence Procedure

Simplified procedures may be applied to low-risk customers. These measures will be applied where there is no suspicion of money laundering, irrespective of any derogation, exemption or threshold, and not necessarily whenever a business relationship is established.

iii – Enhanced Customer Due Diligence Procedure

The Company must apply enhanced customer due diligence measures in situations that, by their nature, may present a high risk of money laundering or terrorist financing.

The Company will take specific and appropriate measures to mitigate the high risk by applying one or more of the following measures:

– Ensuring that the customer's identity is established through additional documents, data or information.
– Applying additional measures to verify or certify the documents provided.

– Ensuring that the first payment for transactions is made through an account opened in the customer’s name. Such account must be held with a credit institution operating in a country that imposes requirements higher than or equivalent to those established by the Company’s regulators.

- d – Verification Procedure

The Company will follow the procedure below to verify the customer’s identity during the establishment of the business relationship:

i – The Company will ensure that the construction of the economic profile, suitability assessment and appropriateness assessment are carried out prior to establishing the business relationship.

ii – Customers have a grace period of fifteen (15) days to provide their identification documents to the Company. During this 15-day period, the Company must ensure the following:

– The cumulative amount of funds to be deposited will not exceed USD 5,000.

– Funds may originate only from a bank account or through other means linked to a bank account in the customer’s name.

– Notification/reminder emails will be sent to customers requesting the customer identification documents.

– The account will be closed where the verification procedure has not been completed after the grace period.

– The Company will not retain any customer funds and accounts will not be frozen unless they are subject to a suspicion of money laundering.

- e – Other Matters Related to Due Diligence

i – Politically Exposed Persons

Politically Exposed Persons (“PEPs”) are persons who have been entrusted with prominent public functions in a foreign country, as well as persons who have a close relationship with politically exposed persons.

The Company must adopt the following additional due diligence measures to determine whether a prospective customer is a politically exposed person:

– Special approval from Senior Management prior to establishing a business relationship with the customer.
– Taking appropriate measures to establish the source of the customer’s assets and the source of funds related to the establishment of the business relationship or transaction.
– Conducting enhanced and continuous monitoring of the business relationship.

ii – Anonymous or Numbered Accounts

The Company is prohibited from maintaining anonymous or numbered accounts. In addition, the Company must pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that favor anonymity. The Company will also take the necessary measures to prevent their use for money laundering or terrorist financing purposes.

iii – Reliance on Third Parties for Due Diligence

The Company is authorized to, and may, rely on third parties to fulfill customer due diligence requirements. However, in such cases, ultimate responsibility for compliance with those requirements will remain with the Company.

5.2 – Customer Account Opening Procedures and KYC Documentation

Before accepting new customers, the Company will require such customers to provide certain information and identification documents.

5.2.1 – Account Opening

- a – Information Required for Account Opening

All prospective customers interested in opening an account with the Company are required to provide certain information, including:

i – Customer personal data.
ii – Construction of the customer's economic profile.
iii – Customer suitability / appropriateness assessment.

Customer identification, including the construction of the economic profile and the suitability / appropriateness assessment, will be carried out before establishing the business relationship with the customer.

- b – Account Opening Procedure

i – The customer completes the account opening forms by providing all required information.
ii – The responsible administrator collects all initial customer information and submits it directly to Senior Management and the Anti-Money Laundering Compliance Officer for examination, review and approval.
iii – Following approval, the administrator records all necessary information in the Company's software systems and communicates it to the relevant departments.

5.2.2 – KYC Documentation

Before accepting new customers and allowing them to trade with the Company, the following documents must be obtained to verify the customers' identities.

- a – The identification documents required from individuals to efficiently implement the Company's KYC procedures are as follows:

i – Proof of Identity

A valid government-issued proof of identity (passport, national identity card, driving licence, etc.) must include the customer’s full name, date of birth, photograph and validity status (expiry date and/or issue date + validity period). It is also ESSENTIAL that the customer take a photograph showing them holding the identity document together with their face, also known as a selfie.

ii – Proof of Residence / Address

A recent proof of address in the person’s name (bank statement, utility bills, telephone bills, etc.) must include the customer’s full name, residential address and issue date (it must not be more than 6 months old).

- b – Legal Persons

A different identification procedure is followed for legal persons (corporate customers) interested in opening an account with the Company.

i – Incorporation Documents

The form and name of corporate documents may vary depending on the country of incorporation and/or the legal form of the company. However, the required government-issued corporate documents must include the corporation’s name, date and place of incorporation, registered office address, directors and authorized signatories, ownership/shareholding structure (shareholders’ names and ownership percentages), and registered corporate activities.

These documents may include, among others, a certificate of incorporation or registration certificate, registered office certificate, certificate of directors and secretary, certificate of registered shareholders, memorandum and articles of association.

ii – Directors’ and Beneficial Owners’ Documents

Personal identification and KYC documents are required for:

– Directors of legal persons.
– Ultimate beneficial owners of the legal person holding 10% or more beneficial ownership.

These identification documents include proof of identity and proof of residence.

iii – Board Resolution

A board resolution of the legal person for the opening of the account and granting authority to the persons who will operate it.

5.3 – Record-Keeping Procedures

The Company must retain the information and documents listed below for use in any investigation or analysis of potential money laundering or terrorist financing by national authorities.

Retention of documents/data, other than original documents or certified true copies maintained in hard copy, may be carried out in other forms, such as electronic format, provided that the Company can retrieve the relevant documents/data without undue delay and present them at any time to the competent authorities upon request. A true translation will be attached where documents/data are in a language other than English.

a – The names and addresses of customers and copies or records of official identification documents (such as passports, identity cards or driving licences).
b – The name and address (or identification code) of counterparties.
c – Details of the account from which funds were paid.
d – The form and destination of payments made by the Company to the customer.
e – Business correspondence.
f – For customer due diligence, copies of supporting evidence must be retained for at least 5 years after the business relationship with the customer has ended.
g – For business relationships and transactions, supporting evidence and records must be retained for at least five years after the transactions have been carried out or after the end of the business relationship.

5.4 – Suspicious Transaction Reporting

A suspicious transaction is a transaction that is inconsistent with a customer's known legitimate business or personal activities, or with the normal business of the specific account, or generally with the economic profile that the Company has established for the customer.

The Company ensures that it maintains adequate information at all times and knows enough about its customers' activities to recognize in a timely manner when a transaction or series of transactions is unusual or suspicious.

5.4.1 – Examples of Suspicious Transactions

Examples of transactions/activities that could constitute suspicious transactions relating to money laundering and terrorist financing include, but are not limited to:

a – Transactions with no discernible purpose or that are unnecessarily complex.

b – Use of foreign corporate accounts, or groups of companies with complicated ownership structures, which cannot be justified based on the customer's needs and economic profile.

c – A large volume of transactions and/or money deposited or credited to an account where the nature of the customer's business activities does not appear to justify such activity.

d – There is no apparent justification for a customer to use the services of a particular financial organization.

e – Frequent transactions in the same financial instrument without an apparent reason and under conditions that appear unusual.

f – Frequent small purchases of a particular financial instrument by a customer who settles in cash, followed by the sale of the total number of financial instruments in a transaction settled in cash, or with the proceeds transferred, at the customer's instructions, to an account other than their own.

g – Transactions that do not conform to prevailing market conditions, particularly in relation to the size and frequency of the order.

h – Settlement of any transaction, particularly a large transaction, in cash and/or through a third party who did not place the order.

i – Settlement of any transaction, particularly large transactions, in cash and/or settlement of the transaction by a third party other than the customer who placed the order.

j – Transfer of funds to and from countries or geographical areas that do not apply, or inadequately apply, FATF Recommendations on money laundering and terrorist financing.

k – Reluctance to provide complete personal information when establishing a business relationship, including information regarding the nature and purpose of business activities, expected account activity, previous relationships with financial organizations, names of officers and directors, or business address.

l – Providing minimal information that is difficult or costly for the Company to verify.

m – Providing unusual or suspicious identification documents that cannot be easily verified.

n – Frequent or large transactions by a customer with no record of past or present employment experience.

o – Introduction of a customer through a foreign financial organization, or a third party whose country/countries or geographical area(s) of origin do not apply, or inadequately apply, FATF Recommendations on money laundering and terrorist financing.

p – Use of an address linked to persons involved in cash transactions, particularly where the same address does not correspond to the declared occupation (e.g., student, unemployed, self-employed, etc.).

q – Shared address for persons involved in cash transactions, particularly where the address is also a business location and/or does not appear to correspond to the declared occupation (e.g., student, unemployed, self-employed, etc.).

r – The customer's declared occupation is not consistent with the level or size of the transactions executed.

s – Use of general nominee documents in a manner that restricts the control exercised by the company's board of directors.

5.4.2 – Suspicious Transaction Reporting Procedure

The procedure for reporting a suspicious customer transaction is as follows:

a – Reports from Company employees in different departments are assessed by the AML Compliance Officer.
b – If deemed necessary, the Compliance Officer will notify the relevant Money Laundering Authorities.
c – After the report is filed, the customer's account(s), as well as any other connected accounts, are closely monitored by the Compliance Officer.
d – After the report is filed, the Company adheres to the instructions given by the relevant Money Laundering Authorities, particularly regarding whether to resume or suspend a particular transaction or keep a particular account active.
e – Electronic transactions executed for the customer are compared and assessed against the anticipated account turnover, the normal turnover from the customer's activities/operations, and the data and information maintained in the customer's economic profile.
f – Significant deviations are investigated and the findings are recorded in the respective customer file.
g – Transactions that are not justified by the information available about the customer are thoroughly examined to determine whether suspicion of money laundering or terrorist financing arises. If so, a report will be submitted to the Compliance Officer and subsequently to the relevant Money Laundering Authorities.

5.5 – Daily / Monthly Procedures of the AML Compliance Officer

The procedure to be followed by the AML Compliance Officer on a daily/monthly basis is as follows:

i – Receive a daily report from staff members regarding any suspicious transaction.
ii – Examine the reports submitted, if any.
iii – Report to Senior Management and advise on the need to take any of the following actions.
iv – Stop transactions if the reports are under review.
v – Inform the customer of the reasons why their transaction was cancelled.
vi – Collect transaction information if the transaction has already been executed.
vii – Report the suspicious transaction to the appropriate authorities as required by law.

6. STAFF EDUCATION AND TRAINING

The Company ensures that its employees are fully aware of their legal obligations under money laundering and terrorist financing prevention laws through a comprehensive employee education and training program.

The training program aims to educate employees about the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

The training program ensures that the Company's employees are fully aware that they may be personally liable for failing to report information or suspicions concerning money laundering or terrorist financing. The timing and content of training provided to employees in various departments are adjusted according to the needs of each department.

The frequency of training may vary according to changes in legal and/or regulatory requirements, employees' obligations and any other changes in the financial system.

The structure of the training program will be aligned with the needs and the various functions of new employees, existing employees and the different departments of the Company.

Ongoing training is provided at regular intervals to ensure that employees are reminded of their duties and responsibilities and kept informed of any developments.

Any personal information collected about the customer, such as name, address, date of birth and contact details, will be maintained by Rocktrading Ltd strictly for business purposes. Other information, such as customer transactions, copies of passports and proof of address, will remain confidential and will be shared only among our account services and compliance departments. In addition, Rocktrading Ltd may inquire into the customer's creditworthiness, which will also remain confidential within our customer files. Such information may be maintained physically or electronically subject to strict access procedures.

Rocktrading Ltd may share customer information with internal departments or affiliated offices that perform marketing, back-office and customer service functions in order to conduct normal business operations. Every employee within Rocktrading Ltd has signed a Confidentiality Agreement, as customer information is required to be kept confidential.

Any questions or requests for additional information regarding our privacy policy may be directed to our Customer Service Department at info@rocktradingltd.com.