RALLYTRADE
DRIVE THE MARKET

ANTI MONEY LAUNDERING POLICY

It is the policy of RallyTrade Limited and its affiliates, (hereinafter “FR") to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. FR is committed to AML compliance in accordance with applicable laws of jurisdictions where FR offers corporate and legal services. FR requires its officers, employees and subsidiaries to adhere to these standards in preventing the use of its products and services for money laundering purposes.

For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

Generally, money laundering occurs in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller’s checks, or deposited into accounts at financial institutions. At the “layering” stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Each employee of FR, whose duties are associated with the provision of products and services of FR and who directly or indirectly deals with the clientele of FR, is expected to know the requirements of the applicable laws and regulations which affect his or her job responsibilities, and it shall be the affirmative duty of such employee to carry out these responsibilities at all times in a manner that complies with the requirements of the relevant laws and regulations.

To ensure that this general policy is carried out, management of FR has established and maintains an ongoing program for the purpose of assuring compliance with the relevant laws and regulations and the prevention of money laundering. This program seeks to coordinate the specific regulatory requirements throughout the group within a consolidated framework in order to effectively manage the group’s risk of exposure to money laundering and terrorist financing across all business units, functions, and legal entities.

Each of the subsidiaries of FR group is required to comply with all aspects of the group’s policy as well as their own AML policies which specifically consider the local AML laws and requirements to which they are subject. Failure by the group and its subsidiaries to comply with the all applicable local AML laws and regulations could result in severe regulatory sanctions, possible fines and criminal penalties and damage to the group’s business reputation.

Risk Assessment

An assessment of the risk of exposure to money laundering issues across all customer relationships shall be completed using the FR standardized risk rating model. The risk rating model shall be approved by the Board of Directors on an annual basis.

Suspicious Activities

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as “red flags.” If a red flag is detected, additional due diligence will be performed before accepting client’s requests or providing services.

Examples of red flags are:

- The customer exhibits unusual concern regarding the AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer’s stated business strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents.

- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.

- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

- The customer makes a funds deposit followed by an immediate request that the money be wired out.

- The customer requests that a deposit/withdrawal be processed in such a manner to avoid the firm's normal documentation requirements.

Customer Identification

FR collects and verifies the personal identification data of our account holders, while logging and tracking itemized statements of all the transactions that are carried out by our clients. Prior to opening an account with FR a valid form of government-issued identification (Driver's License, State ID, or Passport) and bank account information is required, along with your completed account application.

- All FR client funds are held in separate, segregated accounts that are designated only for client deposits and withdrawals.
- FR performs its actions on the basis of the anti-money laundering framework set forth by the Financial Action Task Force.
- FR neither accepts cash deposits nor disburses cash under any circumstances.
- FR does not accept third-party deposits of any kind.
- FR matches each deposit to the account name on file for that customer.
- FR reserves the right to refuse processing a transaction at any stage where it believes the transaction to be connected in any way to money laundering or criminal activity. In accordance with international law, FR is not obligated to inform the client if suspicious activity is reported to any corresponding regulatory or legal bodies.

FR will document and maintain written customer identification procedures ("CIP") that will enable to form a reasonable belief that FR knows the true identity of each customer. If FR is not able to verify the identity of a customer within a reasonable period of time after services or account opening request, that services shall be suspended and account will be closed. Such an account and services will be subject to increased due diligence until such time as the customer's identity has been verified or the account has been closed and services suspended.

CIP for Natural Persons

For natural persons the following information should be obtained, where applicable:

- Legal name and any other names used (such as maiden name).
- Correct permanent address (the full address should be obtained. a Post Office box number is not sufficient).
- Telephone number, fax number, and e-mail address.
- Date and place of birth.
- Nationality.
- An official personal identification number or other unique identifier contained in an unexpired official document (e.g. – passport, identification card, residence permit, social security records, driving license) that bears a photograph of the customer.

FR shall verify this information by at least one of the following methods:

- Confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records).
- Confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority).
- Confirming the validity of the official documentation provided through certification by an authorized person where neccessary (e.g. embassy official, notary public).

CIP for Institutions

The underlying principles of customer identification for natural persons have equal application to customer identification for all institutions. Where in the following the identification and verification of natural persons is involved, the foregoing guidance in respect of such persons shall have equal application. The term institution includes any entity that is not a natural person.
For corporate entities (i.e. corporations and partnerships), the following information should be obtained:

- Name of institution.
- Principal place of institution's business operations.
- Mailing address of institution.
- Contact telephone and email.
- Some form of official identification number, if available (e.g. tax identification number).
- Copy of the Certificate of Incorporation and of the Articles of Association;
- Certified copy of the legal representative's personal ID;

- Copy of the Power of Attorney (if applicable);
- Bank statement (not older than three months);

This information should be verified by at least one of the following methods:

- Undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated.
- Utilizing an independent information verification process, such as by accessing public and private databases.
- Obtaining prior bank references.
- Contacting the corporate entity by telephone, mail or e-mail.
- Recordkeeping
- All identification documentation and services records shall be kept for the minimum period of time required by local law.

Training

All new employees that are responsible with AML policy shall receive anti-money laundering training as part of the mandatory new-hire training program. All employees that are involved in the AML policy are also required to complete AML training annually. Participation in additional targeted training programs is required for all the relevant employees with day to day AML responsibilities.

Administration

For the purposes of AML Policy, FR shall appoint AML Compliance Officer. FR AML Compliance Officer shall be responsible for the administration, revision, interpretation, and application of this Policy. The Policy will be reviewed annually and revised as needed.

The duties of the AML Compliance Committee with respect to the Policy shall include, but shall be not limited to, the design and implementation of as well as updating the Policy as required; training of officers and employees; monitoring the compliance of FR affiliates, maintaining necessary and appropriate records; and independent testing of the operation of the Policy.

Upon notification to the AML Compliance Committee, an investigation will be required to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to suspend activity with the appropriate law enforcement or regulatory agency. AML

Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstance shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.