ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING PROCEDURE MANUAL

Fcorp Services Ltd

Table of Contents

1. INTRODUCTION

Fcorp Services Ltd is registered in the Marshall Islands based on the Marshall Islands Business Corporation Act with registration number […] and regulated by the competent authorities in Marshall Islands. Regarding Anti Money Laundering and Terrorism Financing Procedures the Company establishes measures to detect, prevent and combat money laundering and terrorism financing.

2. PURPOSE

The present manual establishes the means by which anti-money laundering, financing of terrorism and Know Your Client (KYC) guidance is provided in order to achieve full compliance with the applicable legislations and general international standards. The Company aims to adopt such procedures and set adequate practical processes to ensure regulatory compliance, encourage high ethical and professional standards and stop the direct use whether intentionally or unintentionally, of money launderers and terrorism financiers.

3. WHAT IS MONEY LAUNDERING

"**Money Laundering**" Money laundering is the act of concealing the actual source, origin and ownership of money which are obtained illegally. In particular, the term describes the proceeds of criminal activities such as illicit drugs, corruption, organized crime, fraud, sex trade, forgery, illegal logging/fishing, revenue evasion, counterfeit money, piracy, terrorism and other activities which criminals attempt to disguise. Examples can be found in Appendix A.

There are many ways of engaging in money laundering. Some methods may even take place unintentionally and can range from purchase and resale of real estate or a luxury item to passing money through a complex web of legitimate businesses and companies. In most cases, the proceeds of these criminal activities take the form of cash. For this reason, we acknowledge that our Company's products and services may serve as means to those who wish to engage in such criminal activities and thus the Company will implement high-standards to avoid illegal activities.

"**Layering**" Layering is the separation of criminal proceeds from their source by creating complex layering process of financial transactions designed to defeat the audit trail and provide anonymity. It may include telegraphically transferring funds overseas, depositing cash overseas, reselling goods previously with cash.

"**Financing of Terrorism**" Terrorist financing is the act of collecting funds for the provision of terrorist activities. The aim of terrorism is to threaten society, or compel Governments or international organizations. In order to achieve the aforesaid aim, terrorists have to

maintain effective financial infrastructures. For this reason, we acknowledge that our Company's products and services may serve as means to those who wish to engage in such criminal activities and we are committed to playing our role in the fight against terrorism financing.

"**KYC**" Know Your Client (KYC) procedures are means for the Company to identify Clients prior to establishing a business relationship. Such identification methods will usually include requests to provide passport/ ID, residential address, age and other means of profiling the Client accordingly.

4. AML POLICY

Our Company holds the duty to act responsibly and vigilantly when it comes to the prevention of Money Laundering and other criminal activities. The Company is expected by the Anti-Money Laundering Regulations 2002 of the Banking Act. The Policy further aims to avoid assisting the process of laundering and terrorism financing and to counter immediately possible attempts being used for those purposes.

The Company shall establish procedures to obtain appropriate evidence of client identity and shall maintain adequate records of client identity and transactions involved in such a manner as to assist, if necessary, in the investigation of criminal offences.

4.1. Roles and Responsibilities

i. The Company actively opposes any crime or related crime of money laundering and terrorism financing.
ii. The Company will identify the beneficial owner or underlying third party of all established Clients accounts and shall not establish business or maintain the operation of such accounts, unless they are satisfied of this requirement.
iii. The Company will ensure by taking all necessary steps and by following the procedures set on this manual to ensure that accounts are not used to uphold assets derived as a result of, or for enabling the act of any criminal activity.
iv. The Company will from time to time revise and evaluate the efficiency of the present policies and established procedures and methodology in complying with the international requirements and any relevant guidelines, and such evaluation shall be an integral component of any internal audit.
v. The Company is vigilant in ensuring the prevention or misuse in money laundering activities, and will not accept assets or enter into business relationships where there is reason to believe that such assets may have been acquired illegally or that they represent the proceeds of criminal activity.

The Company will keep records of the client's identity and will further maintain adequate records of transactions involved so as to assist the investigation of criminal offences if required.

4.2. The role of the Board

i. The Board holds the responsibility to enforce the Company's AML framework. The Board's role aims to ensure, that the Company acts in compliance with international laws and regulations. The Board in this way is deemed to assist any authority investigation.

ii. The Board and staff are therefore adequately trained to:
    a. Acknowledge the AML and Anti-Terrorist Financing standards in place their staff and the entity it represents;
    b. Reviewing and approving the AML policies and procedures in light of the specific risks faced by the Company. Such considerations will be reflected in the board minutes and noted in the policy;
    c. An individual will be appointed within the organization to ensure that the Company's AML procedures are effectively monitored.

4.3. The role of the Senior Management

i. The Senior management holds the responsibility for the development of risk management programmes and for reporting to the Board on their effectiveness. The designed programmes, should allow the identification of the Client's business pattern of financial transactions and commitments, should be adequately documented and irrespective of whether the Company receives funds from third parties or not, should provide for:
    a. The following internal policies, procedures and controls shall be developed with the guidance of the Senior Management:
        - opening of Client accounts and verification of Client identity;
        - establishment of business with third parties (including custodians, fund managers, correspondent banks, business introducers);
        - establish termination strategy to end unhealthy relationships with existing clients;
        - immediate detection of suspicious activities and immediate reporting on such transactions;
        - maintain internal reporting; and
        - maintain records.
    b. The Senior management further holds the responsibility for the recruitment of some staff, according to the nature and size of the business, to carry out identification, research of unusual transactions and reporting of suspicious activities;
    c. A compliance officer should be designated by the Senior Management to hold an adequate level of authority, seniority and independence so as to coordinate and monitor the compliance program;

d. A training programme shall be designed to confirm that employees adhere to the internal procedures and ensure the familiarity with any dangers they and the business entity may face and any specific to their job responsibilities that can encounter money laundering and terrorist financing risks;
e. Establish procedures that administer information and develop reporting systems that scrutinize customer account activity while enable wider monitoring of substantial balances, as management assets or on a fiduciary level;
f. Establish an independent risk-based function that oversights tests and evaluates any established compliance programs; and
g. Establish screening procedures when hiring employees, and establish ongoing systems that endorse the ethical and professional standards valued by the Company. This should prevent financial institutions from being used as means to carry out criminal activity. In addition, any other personal information of the employee should also be collected and verified according to potential references relating to the individual.

ii. Policies will be reviewed from time to time in order to establish consistency with the business model, product and service offering.

4.4. The role of all employees

All employees:

- Are expected to comply fully with all of the procedures in this Policy.
- Must receive regular trainings, including training detection and reporting of unusual and suspicious activity by clients.
- Are expected to report any unusual or suspicious activity detected ro the Compliance Officer.
- Are expected to understand the law regarding tipping-off and comply with our anti-tipping-off procedures.
- Are expected to cooperate fully with the Compliance Officer and the authorities in the investigation of any possible breaches of the laws and regulations.

4.5. Compliance Officer

The CO is a senior staff member and is responsible for:

- Creating and keeping this manual current
- Monitoring the compliance by our business with the requirements of the laws and regulations
- Monitoring transactions undertaken for Customers

- Identification and management of money laundering risk using our services
- Providing leadership and training on AML & CTF issues to our staff, including new staff
- Investigating unusual matters and reporting those that are suspicious
- Reporting all other matters that must be reported
- Ensuring that our staff know what their responsibilities are
- Monitoring employees in the course of performance of their duties
- Ensuring that our staff are aware of the requirements of this policy, laws and regulations
- Helping out staff where they face problems associated with Customers who they may know
- Overseeing corrective actions where gaps are identified in our operations
- Review this policy periodically for its adequacy

In addition to the Compliance Officer detailed responsibilities mentioned above, the Company appoints a Compliance Officer who is responsible for ensuring the Company's compliance with the international requirements, establish and maintain internal policies, procedures, controls and systems for the following:

- customer identification requirements;
- record keeping and retention requirements;
- monitoring;
- reporting.

The Compliance Officer, is normally a senior member of the Company and holds the responsibility to inform and train employees to identify acts related to money laundering and financing of terrorism. This shall be done by distributing warning notices and updates received from the competent authorities relating to anti-money laundering and combating of financing of terrorism.

Ongoing trainings will be offered to employees as mentioned on the Roles and Responsibilities section above, to ensure that they are up to date with any developments, techniques, methods and trends. The Compliance officer will keep records of the following:

- Who was trained;
- What material they were trained with;
- The attendance logs signed by attendees;
- The date they were trained.

The Compliance Officer is responsible for ensuring that employees are aware and comply with laws and manuals related to money laundering.

5. CUSTOMER ACCEPTANCE PROCEDURES

5.1. Description of the Company's identification and verification process

A Client who wishes to establish a business relationship with the Company is required to follow the below procedure:

5.1.1 The Company is required to establish the identity of the potential client who intends to open an account, engage in any services the Company offers, enters into any type of business relationship with the Company. For this reason clients are expected to provide identification or any similar reliable, independent source document that may signify the identification of the potential Client. The Company will evaluate and verify any identification provided, prior to establishing a business relationship.

5.1.2. The Company will carry out an identification process on:

- An individual engaging on any business transaction
- An individual who acts on behalf of another to conduct a business transaction
- An individual who is alleged to be a beneficial owner
- The Company will assume that the potential client falls in one of the above categories when: an electronic currency transfer is carried out for the client
- A suspicion that the customer is involved in proceeds of crime, a financing of terrorism or a serious offence
- A suspicion that the transaction involves proceeds of crime, or may be used for financing terrorism or for committing a serious offence or
- The adequacy of the customer identification or information is unclear.

The Company will not accept in any way funds from potential clients unless the necessary verification is completed.

5.1.3. In cases where a client engages in any type of business relationship prior to verification, the Company adopts a risk management approach. This approach includes a set of measures on the limitation of the number of transactions that can be performed and further monitoring of such transactions as part of an on-going due diligence process outlines below:

The Company will obtain information on the purpose and nature of the business relationship and the source of the client's funds. The Company will further verify and establish the above by obtaining and cross-checking the:

- potential client's name and address;
- potential client's identity card, social security document, passport or other applicable official identification document;
- potential client's source of funds.

5.1.4. The Company establishes specific procedures for Politically Exposed Persons, defined as individuals who are or have been entrusted with public functions in the Republic of Marshall Islands or in another country or territory, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials including family members or close associates of the politically exposed person.

As such, the Company has appropriate risk management systems to determine if a potential client or beneficial owner is, or is likely to be defined as a politically exposed person. The Company will therefore identify and verify the Client's identity and further obtain the approval of senior management before establishing or continuing a business relationship with the politically exposed person The Company will further take steps to establish the source of funds and source of property and carry out due diligence measures on a more risk sensitive basis. once a business relationship is established, and once the verification of the identity of the customer and beneficial owner is completed to ensure that money laundering risks are managed effectively.

5.1.5. The Company further establishes a Know Your Client (KYC) policy where the exact procedures to be followed are set. The Company will immediately stop any business transaction, if the Client refuses to cooperate with the identification process.

5.1.6. In cases where the client opens another account with the Company, then the Company holds the responsibility to re-verify the identify and address of the said individual. The same is followed when a formerly dormant account has been reactivated or in certain situations where there has been no recent contact or correspondence with the Client within the last 12 months.

5.2. KYC Documentation for natural persons

Prior to accepting new clients and allowing them to trade with the Company, the following documents shall be obtained depending on whether the Client is an individual or a legal entity:

Physical Persons Account

Proof of Identity: A colored scanned copy of the following:

- Valid passport; and/ or
- Valid Identity Card (ID); or
- Driver's license (valid for at least 3 months).

Proof of Address: A colored scanned copy of any of the following:

- A utility bill or bank statement not older than 6 months, stating the client's name and residential address.
  *In cases where the clients are originating from countries where the addresses are identified only by reference to a P.O. Box, a declaration letter signed by an independent government representative or professional officer (such as post office, lawyer, accountant and notary public) confirming the client's address is accepted.
  *In cases where the clients are living with a family member and the only proof of address they can produce is in the name of the relative, a declaration confirming the family relationship is accepted to verify the validity of the proof of address provided.
- The Company may in some cases request copy of the client's credit card in order to ensure that any payments made amount to the specific account of the client and not to any third party.

Legal Persons Accounts

Proof of natural person acting on behalf of the legal entity

- A board resolution authorizing the natural person to act on behalf of the legal entity.
- A passport and utility bill copy of the natural person.

Proof of the legal entity's existence by providing

- Certificate of Incorporation
- Certificate of Good Standing
- Certificate of Registered Office
- Certificate of Directors and Secretary
- Certificate of Shareholders
- Certificate of Incumbency, if applicable (shall replace certificates of incorporation, registered office, directors and secretary and shareholders)
- Memorandum and Articles of Association
- KYC documents for the verification of the identity of the directors/ registered shareholders/ the beneficial owners (passport and utility bill)
- If the legal person is a regulated entity, a copy of the license is needed

Clients are expected to send the requested documents for KYC purposes, within the required timeframe of […] working days to the following address or through the following means:

1. Via email: support@RIMarkets.com

2. Via the Company's website: RIMarkets.com

5.3. Customers' Profile Policy

A Customer Profile Policy is determined and implemented under particular criteria related with clients' risk profile. In particular, the factors that specify the risk category at which a client is attributed are mainly dealing with client:

- The nature of the customer's business (whether cash intensive e.g. casinos and restaurants);
- The nature and frequency of the activity;
- The complexity, volume and pattern of transactions;
- Type, status and value of account;
- Type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place);
- Type of product/ service (e.g. whether private banking, one-off transaction, mortgage);
- Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash withdrawals);
- Geographical origin of the customer;
- Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of money laundering/ financing of terrorism, whether the customer is subject to regulatory or public disclosure requirements);
- Whether the origin of wealth and/or source of funds can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;
- Unwillingness of the customer to cooperate with the financial institution's customer due diligence process for no apparent reason;
- Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

5.3. Risk based approach

The Company's risk-based approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme. This should be evidenced by categorization of the customer base, products and services by risk rating and identification of assigned actions by risk types.

Prior to establishing a business relationship, the Company should assess the potential risk inherent in each new client relationship. This assessment should take into account the products or facilities to be used by the customer and whether and to what extent a customer may expose the Company to risk. The financial institution should then decide whether or not to establish or continue with a relationship.

The Company categorises customers in terms of risk in 3 groups, namely:

- Low Risk
- Medium Risk
- High Risk

The Company's risk based approach take into account customer acceptance and on-going monitoring policies and procedures that assist the Company in identifying the types of

customers that are likely to pose higher than average money laundering and terrorist financing risk.

The Company is required to risk rate all client relationships including those in existence prior to the implementation of these Guidelines. All risk ratings should be documented and should be in place for all customers.

The Company adopted reasonable criteria for assessing the risks (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place).

The Company conducts periodic reviews (however, not more than two years apart) to determine whether any adjustment should be made to its risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

Simplified customer due diligence

Reduced due diligence is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national systems.

Enhanced customer due diligence

A more extensive customer due diligence process should be adopted for higher risk customers. In particular, the Company applies enhanced due diligence to customers where the risk of being used for money laundering or terrorist financing is high. It follows, then, that simplified customer due diligence measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

The Company may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A financial institution may be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries.

Applying a risk-based approach, enhanced due diligence for high risk accounts may include, where deemed relevant, and with more frequency than applied for low risk customers:

a. An evaluation of the principals;
b. A review of current financial statements;
c. Verification of the source of funds;

d. Verification of source of wealth;
e. The conduct of reference checks;
f. Checks of electronic databases;
g. Periodic reporting to the Board about high risk accounts.

The Company should give particular attention to the following business relations and transactions:

a. Where a customer has not been physically present for identification purposes;
b. Correspondent relationships;
c. Business relationships or occasional transactions with a PEP;
d. Business relations and transactions with persons from or in countries and jurisdictions known to have inadequate AML measures;
e. Corporate customers able to issue bearer shares or bearer instruments.

In particular, the Company defines the following types of customers as high risk clients and therefore enhanced due diligence are applied:

a. Non-Face to Face Customers
b. Politically Exposed Persons
c. High-Risk Countries

6. RECORD KEEPING OBLIGATIONS

The Company shall establish and maintain the following records in accordance to the Banking Act on Anti-Money Laundering 2002:

- records of all transactions carried out;
- records that indicate the nature of the evidence obtained, and which comprise either a copy of the evidence or such information as would enable a copy of it to be obtained;
- account files and business correspondence in relation to client accounts;
- client accounts will be kept in the true name of the account holder.

The kept records will also include descriptions on:

- the date and nature of the transaction;
- the type and amount of currency involved;
- the identification number of the account and transaction;
- the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee, if any, the amount and date of the instrument, the number, if any, of the instrument and details of any endorsements appearing on the instrument.

It is the Company's policy to keep records required for a period of at least 6 years from the date the particular business transaction was carried out, or from the date the termination of business relationship took place or accordingly.

The Company will further keep records of any suspicious transaction, suspicious activity or other report. Similarly the Company is expected to keep records of any enquiries relating to money laundering or financing of terrorism made to the Senior Management or Board of Directors. In this way the Company ensures that any records are available for inspection by an authority.

7. REPORTING SUSPICIOUS TRANSACTIONS

The Company will file with the Banking Commissioner, to the extent and in the manner required by this Section 5, a Suspicious Activity Report (SAR) any suspicious transaction that may breach the law or regulation. The Company may also file an SAR regarding any suspicious transaction by completing an SAR form in accordance to the SAR's instructions and collecting and maintaining supporting documentation as required by the Law. The SAR shall be filed with the Banking Commissioner, as indicated in the instructions to the SAR.

The SAR form shall be filed within 3 working days after the date of initial detection by the financial institution or cash dealer of facts that may constitute a basis for filing a SAR.

The Company will further keep records and file with the Banking Commissioner reports of transactions in currency, of a value greater than $10,000 as required by the Anti-money laundering Regulations of the Banking Act 2002.

8. DISCIPLINARY ACTION AND DISMISSAL

The company's staff will face disciplinary action, and possibly dismissal, if they fail to follow this policy, the relevant procedures and requirements. The Company will dismiss any person who is involved in facilitating money laundering, terrorism financing or who launders money or finances terrorism using our products and services, and we will comply with any law that requires us to report such matters.

The Company encourages staff to go to the Compliance Officer if they are unsure or experiencing difficulties within this area.