ANTI-MONEY LAUNDERING AND COUNTER TERRORISM

FINANCING PROCEDURE MANUAL FOR BALTISSE

LIMITED.

Table of Contents

1. WHAT IS MONEY LAUNDERING?

1. Definition

Money laundering is a process of concealing the true origin and ownership of illegally obtained money. Principally, it is proceeds of criminal activities such as illicit drugs, corruption, organized crime, fraud, sex trade, forgery, illegal logging/fishing, revenue evasion, counterfeit money, piracy, terrorism etc.. which criminals attempt to disguise.

2. Money laundering process

There is more than one method of laundering money. Methods can range from purchase and resale of real estate or a luxury item to passing money through a complex web of legitimate businesses and'shell' companies. In most cases, the proceeds of these criminal activities take the form of cash.There are three stages of money laundering, during which there may be numerous transactions made by launderers that could alert us.

3. Placement

Placement is the physical disposal of the cash or asset derived from illegal activity. It includes the opening of numerous bank accounts, depositing cash, exporting cash, and using cash to purchase high value goods such as property or businesses.

4. 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.

5. Integration

Integration provides apparent legitimacy to criminally derived wealth. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re. enter the financial system appearing to be legitimate business funds. This may be achieved through a complex web of transfers or income from apparently legitimate businesses previously purchased with the proceeds of illegal activities.

2. WHAT IS FINANCING OF TERRORISM?

Terrorist financing involves collecting and providing funds for terrorist activity. The primary objective of terrorism is 'to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act'. The goal of the terrorist or terrorist organization is to maintain financial support in order to achieve their aims, and a successful terrorist group, is one that is able to build and maintain an effective financial infrastructure.

Terrorist needs finance for a wide variety of purpose - recruitment, training, travel, materials and

setting up safe havens.

Terrorist control funds from a variety of sources around the world and employ sophisticated techniques to move funds between jurisdictions. In order not to be detected, a terrorist group draws in the service of banks and non banking institutions and takes advantage of their services products

6. Financing Terrorism and Associated activities

If a known terrorist organization conducts or seeks to conduct a transaction via the business (whether or not the transaction or proposed transaction involves cash), such transaction or proposed transaction is deemed to be a suspicious transaction and the business must submit to the International Money-Laundering Information Network (IMoLIN).

3.OUR POLICY

We are expected by the AML & CTF Act to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the institution from being use, intentionally or unintentionally, by money launderers and terrorism financiers.

BALTISSE LIMITED, has adopted an Anti-Money Laundering (AML) Compliance Policy according to the International Money-Laundering Information Network (IMoLIN) standards. Based on the requirement of the above-mentioned Act, BALTISSE LIMITED, is committed to the maintenance of a compliance programme which shall include:-

1. A system of Internal controls and procedures to ensure on-going compliance
2. Internal or external independent testing for compliance
3. Training of personnel in the identification of suspicious transactions; and
4. Designation of an appropriate officer, responsible for continual compliance with the applicable laws

The policies and procedures in this manual implement the duty of vigilance expected of us to avoid assisting the process of laundering and terrorism financing and to react to possible attempts at peing used for those purposes

1. Scope and Objectives of Policy

This policy applies to all BALTISSE LIMITED, ofificers, employees and products and services offered by BALTISSE LIMITED. All business units and locations within TECHNOLOGIES LIMITED, will cooperate to create a cohesive effort in the fight against money laundering. These procedures are established to guide staff in identifying common practices used in money laundering and terrorism financing, to deter such practices and when discovered or suspected, to use a systematic, uniformed approach for dealing with it. All efforts exerted will be documented

and retained. This Policy will be applicable for all operations, local and international. The objective of this policy is to ensure that the products and services of BALTISSE LIMITED, are not used to launder the proceeds of crime and that all of the staff is aware of their obligations and the need for vigilance in the fight against money laundering and terrorist financing. The policy of the

Company: - not to enter into business relationships with criminals and/or terrorists, not to

process transactions which result from criminal and/or terrorist activity and not to facilitate any transactions involving criminal and/or terrorist activity including the financing of terrorism. The Company undertakes to implement all policies and procedures necessary to prevent the money laundering and to comply with all applicable legislation in this regard, such as the regulatory

instructions, laws and regulations issued from time to time regulators of the countries where

BALTISSE LIMITED, operates. The AML Compliance Committee is responsible for initiating

Suspicious Activity Reports (《SARs u) or other required reporting to the appropriate law

enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies

related to the Policy shall be directed to the AML Compliance Committee.

Our AML & CTF Program

Our AML & CTF Program is made up of the contents of this manual. Our activities can be described

as a series of controls to manage the way we:

• Accept applications for transactions;

• Monitor the transactions we do for unusual activity that needs further investigation;

• Identify events that require us to take further action

• Report certain matters to our IMoLIN; and

• Keep records of what we do

2. GENERAL AND SPECIFIC PROVISIONS CONCERNING MONEY LAUNDERING

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 traveler's checks, or deposited into accounts at financial

institutions. At the《integration 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. Both individual employees and the Company itself are liable for criminal conduct if any of the offences below are charged by

authorities. Money Laundering offences can be distributed as follows:

1. Arrangements relating to criminal property - It is an offence to enter into arrangements which will facilitate acquisition, retention or use of criminal property. It is a defense that the employee reported his

knowledge or suspicion to the law enforcement agencies via internal reporting procedures at the first available opportunity.

2. Tipping off - it is an offence to disclose information which is likely to prejudice and

investigation either to the person who is the subject of a money laundering suspicion or any

person other than the law enforcement agencies.

3. Acquisition, use of possession of criminal property - it is an offence to acquire, use or

possess criminal property

4. Handling the proceeds of corruption - corruption by government leaders and public sector officials inevitably involves serious crimes. Not only is there a major reputational risk in handling proceeds from such activities, but criminal charges and constructive trust suits can arise.

5. Failure to report - It is an offence for a person who knows or suspects or has reasonable

grounds for knowing or suspecting that another is engaged in money laundering not to report such

knowledge or suspicion as soon as reasonably practical to the authorities via internal reporting

procedures.

4. CUSTOMER IDENTIFICATION PROGRAM

TECHNOLOGIES LIMITED, has adopted a Customer Identification program. BALTISSE

LIMITED, will provide notice that they will seek identification, collect certain minimum customer identification information from each customer, records such information. Formal identification evidence must be obtained for all new clients conducting transactions with the Company.

Documentation must be from a reputable and identifiable source.

The following information will be collected for all new applications:

1. Their true and full name and if they use more than one, all of their names;

2. Their date of Birth

3. Their occupation

4. Their Permanent Residential Address

5. Passport number and country of issuance

6. Number and country of issuance of any other government-issued document evidencing

nationality or residence and bearing a photograph or other similar safeguard

7.A copy of a government-issued identification (ID Card / Passport)

8. A valid Utility Bill issued on the client's name and current address - not older than 3 months.

Utility bill can be water, electricity bill or adequate bank statements including clients account

number, bank name, name of client and current place of living

9. Their purpose and intended nature of the business relationship with the reporting entity.n addition to identification information as described above, it is essential to collect and record information covering the following for all categories of clients:

1. Source of wealth (description of the economic activity which has generated the net worth)

2. Estimated net worth

3. Source of funds to be invested

4. References or other documentation to corroborate reputation information where available Corporate Customers

Where the applicant company is listed on a recognized or approved stock exchange or where there is independent evidence to show that the applicant is wholly owned subsidiary or subsidiary under the control of such a company, no further steps to verify identity over and above the usual

commercial checks and due diligence will normally be required.

Where the applicant is an unquoted company, it will be subject to a procedure aimed to identify it,confirm its existence, good standing and authority of persons acting on its behalf. Documentation required for such purposes may change depending on each particular jurisdiction and will typically include:

1. Certificate of Incorporation / Certificate of trade or the equivalent, evidencing the company is

indeed incorporated in a particular jurisdiction under the respective registered address;

2. If not available in the Certificate of Incorporation - a document, listing current shareholders of the company

3. Certificate of incumbency or an equivalent document, listing current directors of the company

4. Statutes, Memorandum and Articles of Association or equivalent documents confirming the

authority of the respective officers of the Company to legally bind it.

5. Extract from the Commercial Register of the country of incorporation may also be used to confirm the aforementioned information, if such information is provided in the extract.

VERIFYING INFORMATION

Based on the risk, and to the extent reasonable and practicable, BALTISSE LIMITED, will ensure that it has a reasonable belief of the true identity of its customers. In verifying customer identity, appointed producers shall review photo identification. For verification purposes,

BALTISSE LIMITED, shall rely on a government-issued identification to establish a customer's

identity.

All relevant documentation must ultimately be obtained in the form of originals or copies of the

originals that have been certified by:.

1. A notary public or another authority with equivalent power to certify copies of documents in the relevant jurisdiction; or

2. A relevant state official (judge, police officer, consular official etc) or

3. An authorized financial institution

4. If any document regarding the corporate entity (such as extract from the Commerce Register)is available online through an official website of the relevant state authority, the Company may

refer to such online version of the document, provided that a printout is made by a staff member

of the Company and stored in the respective client file.

It is the responsibility of the MLRO to verify the identity of each new applicant when taking on a new client. The verification procedures must be completed and satisfactory evidence of the new applicant's identity must be obtained before the applicant is sent a customer agreement except in exceptional circumstances (as determined in writing by the Compliance Officer).

Also MLRO will ensure that all clients are checked in the sanction lists, compliance lists via the

automated search program SUM& SUM (). Should the client occurred to be in

any sanction list TECHNOLOGIES LIMITED will not proceed with onboarding such client.

HIGH RISK COUNTRIES

The Company will apply heightened scrutiny to clients and beneficial owners resident in and funds sourced from countries identified by credible sources as having inadequate anti-money laundering standards or representing high-risk for crime and corruption. The Company will apply more

stringent standards to the transactions carried out by clients or beneficial owners domiciled in such

countries.

OFFSHORE JURISDICTIONS

Risks associated with entities organized in offshore jurisdictions are covered by due diligence

procedures laid out in these guidelines. However, the Company will apply more stringent standards

to the transactions carried out by clients or beneficial owners.

HIGH RISK ACTIVITIES

Clients and beneficial owners whose source of wealth is derived from activities known to be

susceptible to money laundering will be subject to heightened scrutiny.

PUBLIC OFFICIALS

Individuals who have or have had positions of public trust such as government officials, senior

executives of government corporations, politicians, political party officials, etc, and their families

and close associates will be subject to heightened scrutiny.

5. COMPLIANCE OFFICER

5.1 Money Laundering Compliance Officer

Name: Robert Briggs

Email Address: support@via.top

1. Roles and Responsibilities

The Compliance officer will be responsible for:.

1. Creating and keeping this manual current;

2. Monitoring the compliance by our business with the requirements of the laws and regulations that relate to AML & CTA

3. Monitoring transactions undertaken for Customers

4. Identification and management of Money Laundering risk using our services

5. Providing leadership and training on AML & CTF issues to our staff, including new staff

6. Acting as a liaison point with the IMoLIN

7. Investigating unusual matters and reporting those that are suspicious to our IMoLIN

8. Reporting all other matters that must be reporting to the IMoLIN

9. Ensuring our staff know what their responsibilities rare

10. Monitoring employees in the course of performance of their duties

11. Ensuring that our staffs are aware of the requirements of this manual and of the AML & CTF Laws and regulations that apply to our business.

12. Reviewing this manual periodically for its adequacy

6. STAFF TRAINING AND AWARENESS

It is essential that everyone in the Company understands what they have to do to comply with the requirements of thic mãnug

All staffs are expected to comply fully with all of the procedures of this manual and are expected to report any unusual or suspicious activity detected to the Compliance officer.

Staff dealing with day to day transactions, are encouraged to consult with the Compliance officer should they feel that a transaction could be considered suspicious for whatever reasons or that a client is behaving or dealing with the Company in a suspicious manner.

All Staffs are expected to understand the law regarding tipping-off and comply with our anti-tipping off procedures

All staffs are expected to cooperate fully with the Compliance Officer and the IMoLIN in the investigation of any possible breaches of the laws that relate to the AML & CTF.

7.MONITORING AND REPORTING

We need to keep records of our business to meet various legal requirements of the Republic of Ireland and ensure all transactions can be readily constructed at any time.

All applications and documents produced to verify identity must be kept for a period of six years after the closure or termination of the account, service or business relationship.

Transaction based monitoring will occur within the appropriate business units of TECHNOLOGIES LIMITED Monitoring of specific transactions will include but is not limited to transactions aggregating USD 5,000 or more and those with respect to which TECHNOLOGIES LIMITED, has a reason to suspect suspicious activity. All reports will be documented.

Where a transaction exceeds the parameters as set out and should client's response be unsatisfactory or cause the Company to form a suspicion, staff are obliged to consult with the Director responsible for that client to document and file a suspicious transaction report.

All Reports made to the IMoLIN must be done with the written authorization of the Director and be discussed with the Company's Compliance Ofificer.

Staff are made aware that a suspicious transaction report made to the TECHNOLOGIES LIMITED must not be disclosed to the client or parties involved in the reported transaction. It must be confidential between the Company and the IMoLIN.

8.SUSPICIOUS ACTIVITY

A suspicious transaction will often be one which is inconsistent with a Customer's know legitimate business. Emphasis will therefore be placed on knowing the customer's business and his/her requirements. It is the responsibility of all staff to report knowledge or suspicion of money laundering.

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 proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee.

Examples of red flags are:

• The customer exhibits unusual concern regarding the Company's compliance with government reporting requirements and the firm's 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 has a questionable background or is the subject of news report 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 engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the government reporting requirements,

especially if the cash or monetary instruments are in an amount just below reporting or recording

thresholds.

• The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

• The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

• The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business

purpose.

• The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

•The customer's account shows an unexplained high level of account activity with very low levels of securities transactions

9. INVESTIGATION

Upon notification to the AML Compliance committee an investigation will be commenced 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, birthdates and address. With the results of the investigation warrant, a

recommendation will be made to the AML Compliance Committee to file a blocked assets and/or a

SAR with the appropriate law enforcement or regulatory agency.

The 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 circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing 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. Confidentiality whilst and investigation is ongoing is of the utmost importance and employees are reminded of the offence of utipping- off u. TECHNOLOGIES LIMITED, has the right to terminate the agreement with the client immediately and to prohibit the client from

withdrawing any assets if the explanations provided are inadequate or in conflict with the AML

Policy.

10. INTERNAL AUDIT

The AML Compliance Committee and the audit functions are segregated to ensure that the

activities of the compliance function are subject to an independent review. The Compliance officer will periodically arrange for this manual to be reviewed by and independent person for compliance and

adequacy. The audit function, should of course, keep the compliance informed of any audit findings relating to compliance. The Compliance Officer cannot do this review, nor can a member of her or his staff. The report of the independent review will be provided to the owner as the Compliance Officer and the Compliance officer will undertake required remediation actions identified in the report if they are practicable and appropriate.