Wealth OBU Ltd
Digital Offshore Bank Unit

Wealth OBU Ltd Compliance program

AML / KYC / CFT Policy

May 2023 vers.2.0

compliance@wealthbank.finance

MWALI
B2020007

ANTI-MONEY LAUNDERING AND COUNTER-**TERRORIST FINANCING POLICY**

Administrative Information:

Legal name:

Wealth OBU Ltd – Wealth Offshore Bank Unit Ltd

Registered address:

IBC Company, Reg. No. HY0121922
BP 1257, Bonovo Road, Fomboni, Island of Mwali (Moheli)
Comoros Union, East Africa.
Class "A" Banking Licence No. B2020007
(Mwali International Services Authority,
M.I.S.A.)

Senior Management – Details:

Director – Massimiliano Arena
Compliance Officer – Fabrizio Pistorino

Wealth OBU Ltd (the Company) is committed to implementing single global standards shaped by the most effective anti-money laundering and counter-terrorism financing standards available in Comoros operated by the Company.

The Company has established an Anti-Money Laundering Program ("AML Program") for this purpose. The objective of this AML Program is to ensure that any money laundering risks identified by Wealth OBU Ltd are appropriately mitigated. This means having adequate systems and controls in place to mitigate the risk of the company being used to facilitate any financial crimes. This policy is designed to represent the basic standards of Anti-Money Laundering and Combating Terrorism Financing procedures and standards, which will be strictly complied to by the Company.

Please note that there may be supplementing policies and procedures established in other documents in support of the Policy referenced in this document, which the Company may implement from time to time This Policy (including any supplementing AML/CFT Procedures) will be periodically reviewed, with timely and suitable changes made as the risks of the business evolve over time.

The purpose of this policy is to provide the basic guidelines to the Company's customers and its staff, irrespective of their location, regarding to essential AML/CFT requirements. To achieve these objectives, and to ensure proper compliance procedures are implemented, the Company will continuously strive to ensure desired Senior Management oversight, appropriate analysis and assessment of the risks exposed to its customers and work/product types, proper systems for monitoring compliance with emphasis on procedures and communications to be adopted, and regular updates to its staff's knowledge and efficiency.

Definitions

“account relationship” means the opening or maintenance of an account by the Company in the name of a person (whether a natural person, legal person or legal arrangement);

“AML/CFT” means anti-money laundering and countering the financing of terrorism;

“Authority” refers to M.I.S.A.;

“beneficial owner”, in relation to a customer of the Company, means the natural person who ultimately owns or controls the customer or the natural person on whose behalf a transaction is conducted or business relations are established, and includes any person who exercises ultimate effective control over a legal person or legal arrangement in the course of carrying on its business of providing a specified payment service;

“connected party” –
(a) In relation to a legal person (other than a partnership), means any director or nay natural person having executive authority in the legal person;
(b) In relation to a legal person that is a partnership, means any partner or manager; and
(c) In relation to a legal arrangement, means any natural person having executive authority in the legal arrangement;

“Customer” or “Client” means a person (whether a natural person, legal person or legal arrangement ("Entity")) with whom the Company establishes or intends to establish an account relationship. These two terms can be used interchangeably;

“FATF” means the Financial Action Task Force;

“legal arrangement” means a trust or other similar arrangement;

“legal person” means an entity other than a natural person that can establish a permanent customer relationship with a financial institution or otherwise own property;

“officer” in relation to the Company that is a legal person refers to any director or any member of the committee of management of the Company;

“STR” means suspicious transaction report;

Table of Contents

Chapter 1

INTRODUCTION

The phenomenon of money laundering, due to its effects and its globalization, can be witnessed through its destabilizing effect on financial markets; it can affect the credibility of financial institutions, both in their relations with regulators and with society in general. Incidents of money laundering, drug trafficking and terrorism financing have increased in recent years, and Wealth OBU Ltd is adopting increasingly stringent standards to combat this scourge.

Wealth OBU Ltd adopts appropriate, sufficient measures aimed to prevent its operations from being used as means to conceal, manage, invest or use any form of money – or other assets – due to illicit activities, or to give the appearance of legality to such activities.

i. Goals and Objectives

Establish the criteria and parameters that the institution must following termsof the design, implementation and operation of a plan for the prevention of money laundering and terrorism financing.

ii. Scope

Wealth OBU Ltd will implement policies and procedures in order to avoid the use of its operations for criminal purposes, as well as to cooperate with global efforts to prevent money laundering and the financing of terrorism. The policies and procedures detailed in this manual intend to provide WB Wealth OBU Ltd .'s staff with the knowledge and resources needed to avoid money laundering and terrorism financing.

Chapter 2

GENERAL PROVISIONS

i. Holder of Comoros Banking License

Wealth OBU Ltd is interested in a safe and legal provision and use of its services and for this purposes, cooperates with local, national and international police and law enforcement authorities.

Wealth OBU Ltd is subject to supervision by the Government of Mwali , Comoro and Financial Transactions and Reports Analysis Centre of Comoro (M.I.S.A.).

MONEY LAUNDERING AND TERRORISM FINANCING OVERVIEW

(https://mwaliregistrar.com/images/PDF/AML%20mwali.pdf)
(https://mwaliregistrar.com/images/PDF/terror.pdf)

i. Money Laundering

Money laundering (ML) refers to the legitimization ('washing') of illegally obtained money to hide its true nature or source. ML involves funds being passed surreptitiously through legitimate business channels by means of bank deposits, investments or transfers from one place (or person) to another. Through the laundering process, illegally obtained funds, or crime funds, are given the appearance of having been legitimately obtained.

ML is a method though which criminals disguise the illegal origins of their wealth - protecting their asset bases - as a means of avoiding the suspicion of law enforcement agencies and preventing leaving a trail of incriminating evidence. The act of laundering is committed in circumstances where a person is engaged in an arrangement (i.e. by providing a service or product), and that arrangement involves the proceeds of the crime. These arrangements include a wide variety of business relationships, e.g. banking, fiduciary and investment management.

Interpol defines ML as, "Any act, or attempted act, to conceal or disguise the identity of illegally obtained proceeds (funds) so that they appear to have originated from legitimate sources."

ii. Terrorism Financing

Terrorism Financing (TF) involves providing finance or financial support to individual terrorists or terrorist organisations. A TF risk comprises three factors: threat, vulnerability and consequence.

Threat: This may be a person or a group of people with the potential to cause harm by raising, moving, storing or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. Threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, as well as individuals or populations having sympathy towards the terrorist organisations.

Vulnerability: This involve areas that can be exploited by the threat or provide support to terrorist activities. Vulnerabilities may include:

- features of a particular sector;
- a financial product or type of service that are easy targets for TF;
- weaknesses in measures specifically meant for TF, or more broadly in AML/CFT systems or controls; or
- jurisdictions with higher risk of TF and ease of raising or moving funds/assets (e.g. large informal economy, porous borders etc).

Consequence: This relates to the impact of a vulnerability. Consequences are effects resulting from the underlying terrorist activity perpetrated through financial systems and impacting the social fabric of the country. These consequences are usually more severe than for ML or other types of financial crime (e.g. tax fraud etc), causing damage including the loss of lives.

Terrorists may move or transfer funds and assets through various methods, including:
• using the financial system to transfer funds;
• relying on systems such as the hawala system in areas with less developed financial system are often employed for multiple small amounts of fund transfers; and
• using international trade networks to transfer assets.

iii. Stages of Money Laundering

Traditionally, it has been accepted that the money laundering process comprises three stages. These stages, while they can be separate and distinct, most frequently occur simultaneously, or often overlap. It all depends on the facilities of the launderer, the requirements of the criminals, and on the robustness, or otherwise, of the regulatory and legal requirements linked to the effectiveness of the monitoring systems of the financial or regulated sector. However, while a convenient way of describing the activity, this three-stage model is a little simplistic, therefore it does not fully reflect what actually happens.

1. Placement: Placing the criminal funds into the financial system directly or indirectly.

At this stage, illegal funds or assets are initially brought into the financial system. This placement makes the funds more liquid. For example, if cash is converted into a bank deposit, it becomes easier to transfer and manipulate. Money launderers place illegal funds using a variety of techniques, which include depositing cash into bank accounts and using cash to purchase assets.

2. Layering: The process of separating criminal proceeds from their source by using complex layers of financial transactions designed to hide the audit trail and provide anonymity.

To conceal the illegal origin of the placed funds, thereby making them more useful, the funds must be moved, dispersed and disguised. The process of distancing the placed funds from their illegal origins is known as layering. At this stage, money launderers use many different techniques to layer the funds. These techniques include using multiple banks and accounts, having professionals act as intermediaries, and transacting through corporations and trusts. Funds may be shuttled through a web of many accounts, companies and countries in order to disguise their origins.

3. Integration: If the layering process succeeds, integration schemes place the laundered proceeds back into the legitimate economy in such a way that they appear to be normal business funds.

Once the funds are layered and distanced from their origins, they are made available to criminals to use and control as seemingly legitimate funds. This final stage in the money laundering process is called integration. The laundered funds are made available for activities such as investment in legitimate (or illegitimate) businesses or spent to promote the criminals' lifestyle. At this stage, the illegal money has achieved the appearance of legitimacy.

It should be noted that not all money laundering transactions go through this three-stage process. Transactions designed to launder funds can also be executed in one or two stages, depending on the money laundering technique being used.

If coordinated successfully, money laundering allows criminals to maintain control over their proceeds and ultimately provide a legitimate cover for their source of income. Money laundering plays a fundamental

role in facilitating the ambitions of the drug trafficker, the terrorist, the organized criminal, the insider dealer and the tax evader, as well as the many others who need to avoid the scrutiny from the authorities that sudden wealth brings from illegal activities. By engaging in this type of activity, it is hoped that proceeds can be placed beyond the reach of any asset forfeiture.

iv. Reasons for Money Laundering

There are several reasons why people launder money. These include:

1. **Hiding Wealth:** Criminals can hide illegally accumulated wealth to avoid its seizure by authorities.
2. **Avoiding Prosecution:** Criminals can avoid prosecution by distancing themselves from the illegal funds.
3. **Evading Taxes:** Criminals can evade taxes that would be imposed on earnings from the funds.
4. **Increasing Profits:** Criminals can increase profits by reinvesting the illegal funds in businesses.
5. **Becoming Legitimate:** Criminals can use the laundered funds to build up a business and provide legitimacy to this business.

v. Social and Economic Consequences of Money Laundering

1. **Undermining Financial Systems:** Money laundering expands the black economy, undermines the financial system and raises questions of credibility and transparency.
2. **Expanding Crime:** Money laundering encourages crime because it enables criminals to effectively use and deploy their illegal funds.
3. **Criminalizing Society:** Criminals can increase profits by reinvesting the illegal funds in businesses.
4. **Reducing revenue and control:** Money laundering diminishes government tax revenue and weakens government control over the economy.

Chapter 4

ENTERPRISE-WIDE RISK ASSESSMENT

An Enterprise-Wide Risk Assessment (EWRA) is intended to highlight the areas where there is an inherent ML/TF risk in the nature of the company's business and operations as a payment service licence holder. The risk assessment must be carried out having regard to the customers, countries or jurisdictions customers are from or in, the countries or jurisdictions the company has operations in and the products and services, transactions and delivery channels of the company. This assessment is essential for determining the systems and controls needed to mitigate the risk of ML and/or TF. The risk assessment will be reviewed at least once every two years or when material trigger events occur. Such material events include (but are not limited to) acquisition of new customer segments or delivery channels or the introduction of new products and services.

The following risk factors have been identified in relation to the business of Wealth OBU Ltd .

i. Country Risk

Wealth OBU Ltd pays particular attention to countries, or geographical locations of operation, which our customers and intermediaries are connected to when these locations are subject to high levels of organized crime, increased vulnerabilities to corruption, and inadequate systems to prevent and detect ML/TF. In conjunction with other risk factors, country risk provides useful information regarding potential money laundering risks.

Each jurisdiction has been labelled with its respective risk level. A jurisdiction may be classified as higher risk due to it being subject to sanctions, embargoes or similar measures. It can also be identified by the Financial Action Task Force ("FATF") as non-cooperative in the fight against money laundering, or identified by credible sources as lacking appropriate money laundering laws and regulations. The jurisdiction is also identified by credible sources as providing funding or support for terrorist activities or having significant levels of corruption, or being a non- transparent tax environment.

WB Payment Inc. does not render financial services to legal entities or individuals of jurisdictions which are identified as high-risk or non-cooperative jurisdictions by the Financial Action Task Force (FATF).

See Appendix 1 for the list of high risk and prohibited countries.

ii. Customer Risk

There is no universal consensus as to which customers pose a higher risk, but, when assessing the customer risk, we consider who our customers are and what they do. We also gather other information that may help us to decide whether the customer is of high risk or not.

<u>Low-risk customers</u>

This category includes the following customers:

A. customer risk factors:

   a) a government entity or a public body in Comoros

b) a corporation listed on a stock exchange and subject to disclosure requirements (e.g. either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

c) an FI incorporated or established outside Canada that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

B. Product, service, transaction or delivery channel risk

a) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme; and

b) financial products or services that provide appropriately defined and limited services to certain types of customers (e.g. to increase customer access for financial inclusion purposes).

C. Country risk factors:

a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT Systems; or

b) countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity

Medium-risk customers

This category includes the following customers:

A. Public companies listed on stock exchanges in countries which inadequately apply FATF recommendations;

B. Private companies that are not classified as high-risk; and

C. Any other customer not falling under either high-risk or low-risk category.

In the above cases, Wealth OBU Ltd should gather sufficient information to establish whether the customer qualifies to be classified as a medium-risk customer and perform Customer Due Diligence and Identification Procedures.

High-risk customers

This category includes the following customers:

A. customer risk factor

a) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between Wealth OBU Ltd and the customer);

b) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;

c) companies that have nominee shareholders or shares in bearer form;

d) cash intensive business;

e) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business

f) the customer or the Beneficial owner of the customer is a PEP.

g) Customers who are not physically present for identification purposes (non-face-to-face Customers)

h) Customers convicted for a Predicate offence

i) Customers from countries which inadequately apply FATF's recommendations

j) Other Customers that their nature entail a higher risk of ML/TF

k) Any other customer determined by Wealth OBU Ltd itself to be classified as such.

B. product, service, transaction or delivery channel risk factors

a) anonymous transactions (which may involve cash); or

b) frequent payments received from unknown or un-associated third parties.

C. country risk factors:

a) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT Systems;

b) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;

c) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operation

d) high risk countries identified as such by the FATF

In the above cases, Wealth OBU Ltd should gather sufficient information to establish whether the customer qualifies to be classified as a high-risk customer and perform Enhanced Customer Due Diligence and Identification Procedures (see Chapter 5 VII).

iii. Business Nature Risk

The nature of Wealth OBU Ltd 's business involves transmission of monies and this inherently will result in ML/TF risks. The ML/TF risks increase where transmission of monies is carried out on a cross-jurisdictional basis. CDD measures will be conducted on each customer.

The Company will identify its customers and verify the submitted documents using means of Artificial Intelligence by an external third-party vendor, such as Ondato.

Chapter 5

RISK MANAGEMENT FRAMEWORK

As identified above, the major risks of the company's business are country risk, customer risk and business activity risk.

The online nature of the company's business and the speed with which the transfer of funds can be affected are also factors that affect the company's risk exposure. The company has identified key risk areas based on which it will accord appropriate risk ratings to customers. The company will implement measures to mitigate the risks associated with prospects and customers with higher risk ratings.

The basic elements of the company's risk management framework are as follow:

i. Know Your Customer (KYC)

The "Know Your Customer" procedure is the most effective weapon against being used unwittingly to launder money and finance terrorism. Know Your Customer (KYC) is the process of a business identifying and verifying the identity of its customers. The objective of KYC guidelines is to prevent financial institutions from being used, intentionally or unintentionally, by criminal parties for money laundering activities. Related procedures also enable these institutions to better understand their customers and their financial dealings. This helps them to manage their risks prudently. Compliance with AML, Know Your Customer ("KYC") and sanctions requirements continues to be a key focus area for management, and the company is taking all necessary steps and precautions to ensure that it is following appropriate compliance procedures to meet the increasing regulatory demands.

The requirement to verify the identity of an individual and confirm the existence of a corporation or of an entity other than a corporation under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations applies to all reporting entities (REs).

KYC controls typically includethe following:

- Collection and analysis of basic identity information ("Customer Identification Program" or CIP)
- Name-matching against lists of known parties (such as "politically exposed persons" or PEPs)
- Name-screening against sanctions lists
- Determination of the customer's risk in terms of propensity to commit money laundering, terrorism financing, or identity theft
- Creation of an expectation of a customer's transactional behaviour
- Monitoring of a customer's transactions against expected behaviour and recorded profile, as well as that of the customer's peers
- Having a properly defined and practiced KYC Policy
- Identification of customers with inappropriate intentions to help to detect suspicious activity in a timely manner, preventing money laundering or terrorist financing
- Promotion of compliance with all regulations
- Promotion of safe and sound money transfer practices
- Minimization of the risk of services being used for illicit activities
- Protection of the company's reputation

ii. Customer Due Diligence

Customer due diligence (CDD) forms an integral part of a global effort to combat money laundering, terrorist financing and fraudulent activities. Under this approach, Wealth OBU Ltd will collect information upon account opening, as well as on a periodic basis and from time to time, as required, to identify our customers and develop an understanding of their normal, expected banking activities.

Every Customer, including its beneficial owners, connected parties and natural persons appointed to act on behalf of, will be subject to background screening against relevant money laundering and terrorism financing information sources, as well as lists and information provided by the Authority or other relevant authorities in Comoro for the purposes of determining if there are any money laundering or terrorism financing risks in relation to the customer.

Business relationships

Wealth OBU Ltd shall identify and verify identity of customers prior to establishing a business relationship with them. A business relationship is a relationship established between Wealth OBU Ltd and a client to conduct financial transactions or provide services related to financial transactions. As per definition from M.I.S.A., the company will be considered as entering into a business relationship with a client when one of the following occurs:

- The Company enters into a service agreement with a client to provide payment services;
- Account opening for a client;
- When a client does not hold an account with Wealth OBU Ltd , but for the second time within a 5 year period, engages the Company in a financial transaction for which the Company is required to verify the client's identity.

iii. Customer Risk Assessment

The risk level is determined in two steps:

- A scoring process based on objective or quantifiable criteria, which can be automated or delegated to a KYC team
- The consideration of qualitative elements requiring an analysis or judgement, as well as consideration of objective factors that are not taken into account at all in the scoring grid calculation, or not fully taken into account in the scoring grid calculation
- A customer risk level is associated with every Customer and determines the level of due diligence related to the information collection, the onboarding or recertification decision process, and the recertification frequency.
- There are two levels of Due Diligence: Regular Customer Due Diligence (CDD) and Enhanced Customer Due Diligence (EDD).
- Low or Medium risk customers are subject to CDD.
- High risk customers are subject to EDD.

iv. Scoring System

See Appendix 3 and 4 for the risk assessment for corporate customers as well as individual customers. Depending on the score attained by each customer, the customer will be classified into different risk categories accordingly.

v. Scoring Criteria

Corporate customers

- Low risk: Below 10 points
- Medium risk: Between 11 to 20 points
- High risk: Above 21 points

Individual customers

- Low risk: 0 points
- Medium risk: 2 points
- High risk: Above 2 points

vi. Regular Customer Due Diligence

Individual Account

For a customer that is a natural person, Wealth OBU Ltd should identify the customer by obtaining at least the following identification information:

a) full name;

b) date and place of birth;

c) nationality

d) unique identification number (e.g. identity card number or passport number) and document type.

e) Residential address

In verifying the identity of a customer that is a natural person, Wealth OBU Ltd should verify the:

a) full name, including any aliases; and

b) date of birth;

c) unique identification number and document type of the customer;

d) residential address;

by reference to documents, data or information provided by a reliable and independent source, examples of which include:

a) Canada identity card or other national identity card;

b) valid travel document (e.g. unexpired passport); or

c) a utility bill

d. other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

The identification document obtained by Wealth OBU Ltd should contain a photograph of the customer. In exceptional circumstances where Wealth OBU Ltd is unable to obtain an identification document with a photograph, Wealth OBU Ltd may accept an identification document without a photograph if the associated risks have been properly assessed and mitigated.

Corporate Account

Where the customer is a legal person Wealth OBU Ltd is required to identify and screen all the connected parties of a customer. However, Wealth OBU Ltd may verify their identities using a risk-based approach. Wealth OBU Ltd shall identify connected parties and remain apprised of any changes to connected parties. Identification of connected parties may be done using publicly available sources or databases such as company registries, annual reports or based on substantiated information provided by the customers.

Wealth OBU Ltd shall, identify the connected parties of the customer, by obtaining at least the following information of each connected party:

a) full name, including any aliases; and

b) unique identification number (such as an identity card number, birth certificate number or passport number of the connected party).

In relation to trust and similar legal arrangements, Wealth OBU Ltd shall perform CDD measures on the customer by identifying the settlors, trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristics or class) and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership), as required by paragraph 7.14 of the PSN01 Notice.

In verifying the identity of a customer that is a legal person or legal arrangement, Wealth OBU Ltd should normally verify

a) Name, legal form, proof of existence and constitution based on certificate of incorporation, certificate of good standing, partnership agreement, trust deed, constitutional document, certificate of registration or any other documentation from a reliable independent source; and

b) Powers that regulate and bind the legal person or arrangement based on memorandum and articles of association, and board resolution authorizing the opening of an account and appointment of authorized signatories.

vii. Enhanced Customer Due Diligence

Wealth OBU Ltd applies Enhanced Customer Due Diligence (EDD) to customers categorized under high risk. These customers are subject to additional due diligence in addition to that required for CDD. This higher level of due diligence is required to mitigate the increased risk. Crucial to the integrity of the company's EDD process are the reliability of information and information sources, and the type and quality of information sources used, as well as the deployment of properly trained analysts who know where and how to look for information, and how to corroborate, interpret and decide upon results.

What the EDD procedure actually entails is dependent on the nature and severity of the risk. The additional due diligence could take many forms, from gathering additional information to verify the customer's identity or income source(s), or perhaps an adverse media check. These checks should be relative and proportionate to the level of risk identified, providing confidence that any risk has been mitigated, and that the risk is unlikely to be realized.

One or more of the following enhanced customer due diligence (EDD) measures may be taken in order to manage and mitigate the ML/TF risk that is higher than usual:

- Obtain additional identification documents, data or information from credible and independent source.
- Gather additional information or documents on the purpose and nature of the business relationship.
- Gather additional information or documents for the purpose of identifying the source of funds and wealth of the customer.
- Gather information on the underlying reasons of planned or executed transactions.
- Increasing the number and frequency of control measures in monitoring customer relationships and/or transactions.
- Receiving permission from the senior management to establish or continue a business relationship.

Approval must be obtained from the company's Board of Directors before establishing or continuing an account relationship with the high-risk customer or undertaking any transaction for the high-risk Customer. The Board of Directors shall provide and record written reasons for its decision as to whether to approve or reject a high-risk customer.

viii. Ongoing Monitoring

Wealth OBU Ltd will conduct periodic ongoing monitoring whenever a business relationship is established with a client. Clients of lower risk categories will be subject to less frequent ongoing monitoring while high- risk clients will be subject to enhanced ongoing monitoring.

High-risk customers: Every 1 year

Medium-risk customers: Every 2 years

Low-risk customers: Every 3 years

In addition to the above periodic reviews, existing CDD records should be reviewed upon trigger events. Examples of trigger events include:

- Re-activation of a dormant account.
- Change in the beneficial ownership or control of the account.
- When a significant transaction is to take place.

- When a material change occurs in the way the customer's account is operated.

If an account relationship is established or maintained with a high-risk customer, enhanced monitoring must be undertaken throughout the course of the relationship. The degree and nature of monitoring of the account relationship and transactions undertaken for the customer must be increased accordingly, to help assess whether the customer's conduct is in any way unusual or suspicious.

The Company will keep records of the measures taken and information obtained from the ongoing monitoring of clients. This includes the processes in place to perform ongoing monitoring, processes in place to perform the enhanced ongoing monitoring of high-risk clients, processes for recording the information and information obtained as a result of ongoing monitoring.

In the event EDD is unable to be performed, the company will not open the account or commence business relationship or perform the transaction. In the event a business relationship is already established, the Company will terminate the business relationship. In addition, the Company and Compliance Officer will consider making a suspicious activity report in relation to the customer.

ix. Politically Exposed Persons

Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with prominent political profile or holding senior public office. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption.

However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.

A domestic PEP is a person who currently holds, or has held within the last 5 years, a specific office or position in or on behalf of the Comoro federal government, a Mwali provincial (or territorial) government, or a Comoro municipal government. Specifically, the person has held the office or position of:

- Governor General, lieutenant governor or head of government;
- member of the Senate or House of Commons or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;
- head of a government agency;
- judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- leader or president of a political party represented in a legislature; or
- mayor.

A foreign PEP is a person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

- head of state or head of government;
- member of the executive council of government or member of a legislature;

- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a state-owned company or a state-owned bank;
- head of a government agency;
- judge of a supreme court, constitutional court or other court of last resort; or
- leader or president of a political party represented in a legislature.

In the event a customer or any beneficial owner of the customer is determined to be a PEP or a family member or close associate of a PEP, Wealth OBU Ltd will end business relationships immediately.

In order to identify any Politically Exposed Persons ("PEPs") among the related persons (UBO, Senior Managing Officials, Directors, Authorized Signatories, Guarantors), and any sanction (affecting either the entity/legal person itself, its parent companies, its related persons, its country of incorporation/registration, its location, or its countries of activity or tax residence), the following checks are mandatory at on-boarding and recertification.

Chapter 6

KNOW YOUR EMPLOYEES

There has been a lot of attention regarding 'Know Your Customers" policies and procedures. In accordance with this, Wealth OBU Ltd has, indeed, concentrated on identifying its customers. However, the company believes on doing the same with employees. Financial crime investigators generally agree that 4% of an institution's workforce has been caught embezzling and never prosecuted.

i. Staff Screening and Integrity of Staff

Staff Screening

The best way to reduce insider abuse is to stop it before it starts. It starts during the hiring process, with the company exercising the same precautions as it does when opening an account. The company performs due diligence on employees and screens employee names through World Check and verifies any information supplied.

Integrity of Staff

Integrity is one of the fundamental values that employers seek in the employees that they hire. Employers, business leaders and employees can benefit from integrity in the workplace. Integrity involves moral judgment and character, honesty and leadership values. Individuals who show integrity in the workplace not only understand right from wrong, but they practice it in all they do. This is beneficial in a business environment, where trustworthy actions set the foundation for successful business relationships.

Counterchecking of Work Completed by Staff

The company performs occasional spot checks on work done by staff at all levels. Usually, these checks are undertaken by senior management to ensure that the company's policies and procedures are being followed and everything is in the correct order.

Actions to Help to Get to Know its Employees

1. A criminal conviction search in jurisdictions where it is possible
2. Credit checks
3. Conducting a private investigation, if thought necessary
4. An internet check before they are hired

ii. Staff Training for the Awareness of AML/CFT

The company will provide periodical anti-money laundering and countering terrorism financing training to the employees. Staff will be made aware of their own personal legal obligations/responsibilities under the regulations, and that they can be personally liable for failure to report information to the authorities. The company must ensure sufficient guidance is given to employees to enable them to form suspicion or to recognize when money laundering/terrorist financing is taking place, taking into account the nature of the transactions and instructions that staff are likely to encounter, the type of product or service, and the

means of delivery (i.e. face-to-face or remote). This will also enable staff to identify and assess the information that is relevant for judging whether a transaction or instruction is suspicious in the circumstances. The training will be conducted at least once every six months.

The training will be in writing, reviewed and kept up to date. The training program will be delivered and tailored to employees who:

- Have contact with clients such as front-line staff or agents;
- Are involved in client transaction activities;
- Handle cash or funds in any way;
- Are responsible for implementing or overseeing the compliance program.

The training will include the following:

- AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;
- prevailing techniques, methods and trends in money laundering and terrorism financing; and
- the company's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of employees and officers in combating money laundering and terrorism financing.

As and when a new product, services or delivery methods are taken on-board, the Company will conduct a training for all its employees to go through the methodologies, various ML/TF risk associated with the service and the reporting requirements.

In order to ensure that the AML training is given sufficient prominence a register will be kept of all training received by an employee. This is to be regularly updated and will be overseen by the Compliance Officer.

If a meeting with all employee is not possible, the relevant managers/senior team members will ensure that they have a one on one training with the employee following which a documented record will be kept.

The company will apply necessary processes and controls for managing instances when an employee is non-compliant with the requirements of the AML/CFT Program. Upon identifying employee being non-compliant, the company will undertake the following steps which include but are not limited to.

- Additional training
- Written warnings, suspensions and instant dismissal depending on the degree of non-compliance.

iii. Essential Training for Employees

- Knowledge of company policies and procedures
- Learning how to identify suspicious activity and structured transactions
- Learning procedures for verifying customer identity
- Familiarity with anti-money laundering policies
- Knowledge of record-keeping and reporting requirements

iv. Effectiveness Review

Wealth OBU Ltd will conduct an effectiveness review at least once every two years to test the effectiveness of the elements of the compliance program. This is to ensure that the company does not have any gaps or weaknesses within the compliance program and that the company is effectively detecting and preventing ML/TF. This shall be conducted by an internal or external auditor. In the event an internal or external auditor is not engaged, a senior management team officer who has prior working knowledge on AML/CFT will conduct the effectiveness review. The Director will report to M.I.S.A. in writing no later than 30 days after the effectiveness review is completed.

Examples of effectiveness review include:

- Interviews with those handling transactions to evaluate their knowledge of policies and procedures and related record keeping, client identification and reporting obligations.
- A review of the company's criteria and process for identifying and reporting suspicious transactions.
- A sample of the company's account opening records followed by a review to ensure that client identification policies and procedures are being followed.
- A sample of large cash transactions followed by a review of the reporting of these transactions.
- A sample of electronic funds transfers followed by a review of the reporting of these transactions.
- A sample of clients followed by a review to see if the risk assessment was applied correctly.
- A sample of clients followed by a review to see if the frequency of your ongoing monitoring is adequate.
- A sample of high-risk clients followed by a review to ensure that enhanced mitigation measures were taken.
- A review of a sample of records to ensure proper record keeping procedures are being followed.
- A review of risk assessment to ensure it reflects your current operations.
- A review of policies and procedures to ensure they are up-to-date with the current legislative requirements.

Chapter 7

INTERNAL CONTROL STRUCTURE

i. Duties and Responsibilities of the Compliance Officer

The function of the Compliance Officer does not mean that other employees are exempt from the obligation to detect, and internally report, any unusual operations. Other employees must diligently follow the company's functions related to the prevention and control of ML/FT.

- Making sure the business complies with its AML/CFT obligations;
- Reporting regularly to the Board of Directors and senior management about how the business is meeting its obligations, including alerting them if the business is not complying.
- Taking day-to-day responsibilities to ensure the business is legally compliant while being exposed to minimal ML/TF risks;
- Helping to create, implement and maintain internal policies, procedures and systems for AML/CFT compliance.
- Being the contact point for the company's dealing with M.I.S.A., for example submitting STR;
- Addressing any feedback from M.I.S.A. or internal auditors about how the company is managing its risks or about the AML/CFT Program;
- Provide periodic training to employees to ensure they are aware of company policies and procedures;
- Manages the KYC files of Customers and monitors the file completion and integrity of information;
- Reviewing, approving and signing the Risk Assessment Report;
- Coordinating the decision process as to whether to onboard a Customer.
- Preparing and attending the M.I.S.A. examination which can be on-site or desk examination.

The Compliance Officer will hold a sufficiently senior position within the organizational structure in the company. Wealth OBU Ltd has ensured that the reporting lines between the customer service staff and the Compliance Officer is as short as possible to ensure speed, confidentiality and accessibility of information.

Chapter 8

RECORD-KEEPING AND MAINTENANCE OF RECORDS

Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assist the court to examine all relevant past transactions to assess whether the property or funds are the proceeds of, or related to, criminal or terrorist offences. Wealth OBU Ltd will maintain customer transactions and other records that are necessary and sufficient to meet the record-keeping requirements under the Compliance Officer and the Authority, appropriate to the scale, nature and complexity of its business.

The company follows closely to the record keeping guidelines from M.I.S.A.. The company will keep records in such a manner that they can be provided to M.I.S.A. within 30 days of request. The records will be kept in a machine-readable or electronic form. The below records will be kept for at least 5 years.

i. Preserved Documentation

The company will keep the following reports:

- Reports – a copy of every report sent to M.I.S.A.
    - Suspicious Transaction Reports
    - Terrorist Property Reports
    - Large Cash Transaction Reports
    - Large Virtual Currency Transaction Reports
    - Electronic Funds Transfer Reports
- Large cash transaction records
    - WBs must keep a large cash transaction record when they receive $10,000 or more in cash.
- Large virtual currency transaction records
    - WBs must keep a large virtual currency (VC) transaction record when they receive VC in an amount equivalent to $10,000 or more.
- Records of transactions of $3,000 or more
    - When the company receives $3,000 or more in funds or an equivalent amount in VC for the issuance of traveller's cheques, money orders or other similar negotiable instruments from a person or entity.
- Records of remitting and transmitting $1,000 or more in funds by means other than an electronic funds transfer
    - When the company transmits $1,000 or more in funds at the request of a person or an entity by means other than an electronic funds transfer (for example, by using informal value transfer systems such as Hawalas)

- Records of electronic funds transfers of $1,000 or more
- Records of virtual currency transfers equivalent to $1,000 or more
- Foreign currency exchange transaction tickets
- Virtual currency exchange transaction tickets
- Created or received internal memorandums about the Companies Act 2014 services,
- Service agreement records

SUSPICIOUS TRANSACTION REPORTING (STR)

i. What is a Suspicious Transaction?

A transaction may be of suspicious nature irrespective of the amount involved. A suspicious transaction involves there being reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. Suspicious transactions involve a case of there being any information, suspicion or reasonable grounds to suspect that the asset – which is subject to the transactions being carried out, or attempted to be carried out – has been acquired through illegal means (or used for illegal purposes) and is used, in this scope, for terrorist activities, or by terrorist organizations, terrorists or those who finance terrorism.

ii. Transaction-related

- Transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale, e.g. a customer makes frequently purchases at a high price and subsequently sells at a considerable loss to the same party.
- Transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business, e.g. a customer makes multiple small deposits/withdrawals to avoid currency reporting requirements.
- Where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged, e.g. the size and frequency of a customer's trades unexpectedly appear to be large and active while the previous pattern has been small and inactive.
- Transfers to and from high risk jurisdiction(s) without reasonable explanation, which are not consistent with the customer's declared business dealings or interests.
- Routing of funds or cryptocurrencies through third party service provider, e.g. cryptocurrency tumbler (also known as cryptocurrency mixing services) by obscuring the transaction details and making it difficult to track their original source.

iii. Customer-related

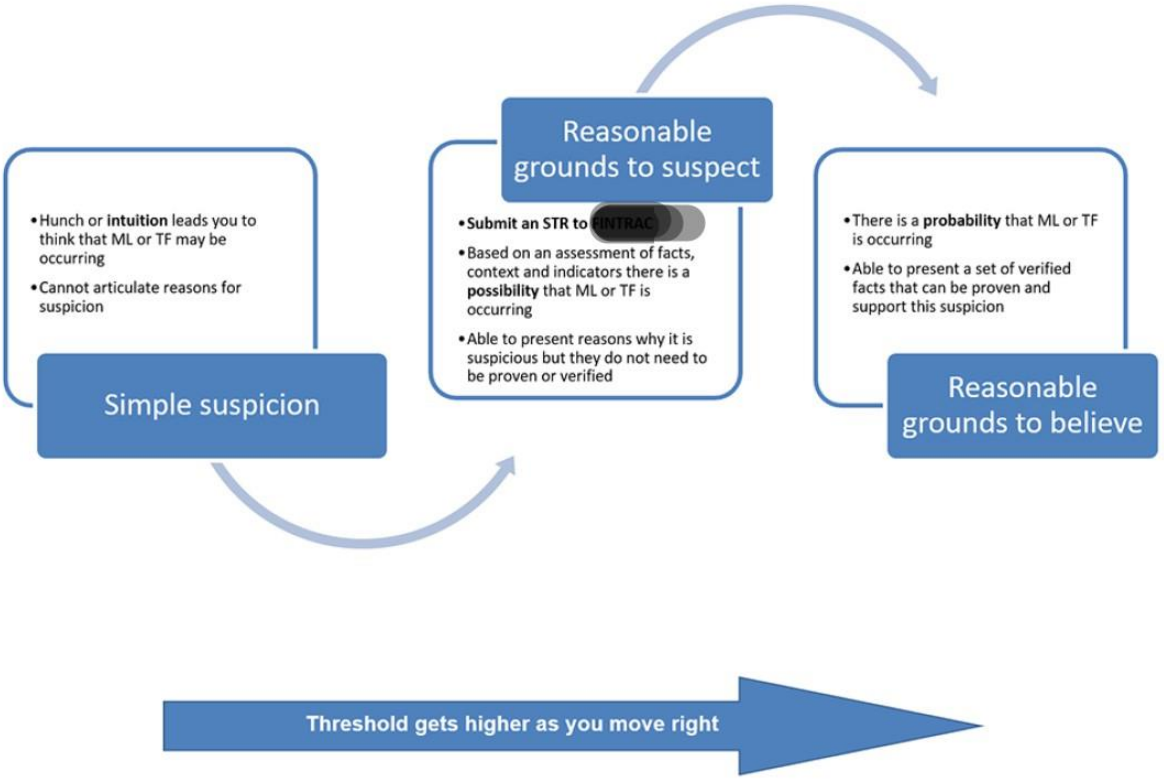
- Where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process.
- Where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation.
- A customer was introduced by someone or an entity that is based in high risk jurisdiction(s).
- A customer uses a bank account, telephone number, or mailing address that is located in high risk jurisdiction(s).
- A customer has opened multiple accounts for no apparent business reason.

iv. Employee-related

- Changes in employee characteristics, e.g. lavish lifestyles or avoiding taking holidays without reasonable cause.
- Unusual or unexpected increase in the sales performance of an employee.
- The employee's supporting documentation for customers' accounts or orders is incomplete or missing.
- The use of an address which is not the customer's home or office address, e.g. utilization of an employee's address for the dispatch of customer documentation or correspondence.

v. Reporting Suspicious Transactions

In the event the company faces a suspicious transaction with Reasonable Grounds to Suspect (RGS), the Compliance Officer will at the soonest file a STR with M.I.S.A.



APPENDIX 1- HIGH RISK (AND PROHIBITED) COUNTRY LIST

Grey list contains jurisdictions which have strategic deficiencies in their regimes to counter money laundering, terrorist financing and proliferation financing.

WB Payment Inc. shall consider in its risk analysis the information presented for each country under the grey list.

https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html#pakistan

As of 4th March 2022, Grey list consists of 18 jurisdictions:

1. Albania
2. Barbados
3. Burkina Faso
4. Cambodia
5. Cayman Island
6. Haiti
7. Jamaica
8. Jordan
9. Mali
10. Malta
11. Morocco
12. Myanmar
13. Nicaragua
14. Pakistan
15. Panama
16. Philippines
17. Senegal
18. South Sudan
19. Syria
20. Turkey
21. Uganda

22. United Arab Emirates

23. Yemen

Black list contains high-risk jurisdictions which have significant strategic deficiencies to counter money laundering, terrorist financing and proliferation financing.

For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country.

As of 21st of February 2020, Black list consists of 2 jurisdictions:

1. Democratic people's republic of Korea
2. Iran

APPENDIX 2- HIGH RISK (AND PROHIBITED) INDUSTRY LIST

Auction houses
Arts and antiques (sculptures, statues, antiques, collector's items, archeological pieces)
Second-hand goods sale
Fast-Moving Consumer Goods (FMCG), Wear, Shoes, Dishes
Retail distribution (supermarkets, tobacco, restaurants, gasoline and service stations, mobile phones, computer equipment, jewelries)
Alcohol and Tobacco wholesales or production
Production or trade in weapons and munitions, arms and defense
Precious stones & precious metals
Production or trade in radioactive materials and nuclear material
Equipment for renewable energy
General and specialized construction contractors
Metallurgy, Chemicals and Allied Products, Oil & Gas
Pharmaceuticals
Trade in wildlife or wildlife products regulated under CITES
Trading of Animal Fur and Fur products
Production or trade in pesticides and agrochemicals /fertilizers
Car, Boat, Airplane Dealers
Other Manufacturing or Distribution
Precious stones & precious metals, Uranium
Oil & Gas
Quarries, other mining & extraction of iron ores or coal
Pawn brokers, microfinance, crowdfunding
Unlicensed trading in Derivatives/Options/Hedging/FOREX
Political organizations I Parties
Unlicensed gaming (incl. Internet, casinos, betting shops) and Gambling, unlicensed casinos and equivalent enterprises: Betting/Horse Racing/Bingo/Sports/ Online Betting/ Online Casino/Online Poker/Online Gambling/Online Betting
Trust and offshore company services, domiciliation services
Real Estate Agents I agencies
Real Estate Development and Construction
Religious organizations I NGOs or Charities
Night clubs
Automotive repair services
Garbage I waste management I environmental clean-up
Laundromats
Professional sports clubs, agents and intermediaries
Highly labor-intensive agriculture (vineyards, fruits, vegetables, sugar cane)
Healthcare (private clinics, residential activities)
Travel agencies, custom brokers
Attorneys, tax advisers
Training providers

APPENDIX 3- RISK ASSESSMENT REPORT FOR CORPORATE CLIENTS

CLIENT NAME:				
Risk Parameter	**Description**	**Description**	**Weight (0 to 3)**	**Comments**
Geographical Risk				
Country of Incorporation (low-risk countries)?	Yes/No	If the answer is Yes, the score will be 0		
If answer to above is no, what country is the company incorporated?		If the company is incorporated in a jurisdiction that is sanctioned, the risk will be 3.		
Business Risk				
Date of creation		If the company is incorporated less than 1 year ago, the score will be 2. Otherwise, the score will be 0		
Countries of Activity		If the company has more than 5% of activities in Major Sanctioned countries, the score will be 3. If the company has less than 5% of activities in Major Sanctioned countries, the score will be 2. If the company has no activities in Major Sanctioned countries, the score will be 0		
Sector of Activity		If the company is in any sectors listed in		

		Appendix 1, the score will be 3. Otherwise, the score will be 0.		
Declared Monthly Turnover		If the declared monthly turnover is above CAD 10,000,000, the score will be 3. If the declared monthly turnover is above CAD 2,500,000, the score will be 2. If the declared monthly turnover is below CAD 2,500,000, the score will be 0.		
Sanctions		If there are sanctions involved, the score will be 3.		
Financial Security Incidents		If there is at least one financial security incident in last 5 years, the score will be 3. Otherwise, it will be 0.		
Declared Partners				
Countries of Activity (Sensitive Countries)		If the company has partners with more than 5% of activities in Major Sanctioned countries, the score will be 3. If the company has partners with less than 5% of activities in Major Sanctioned countries, the score will be 2.		

		If the company has partners with no activities in Major Sanctioned countries, the score will be 0		
Sanctions		If the partners are involved with sanctions, the score will be 3.		
UBO				
UBO residence(s)		If the UBO is a resident of sanctioned country, the score will be 3.		
Presence of PEP		If the UBO is a PEP, the score will be 3.		
Sanctions		If the UBO is involved with sanctions, the score will be 3.		
SUMMARY:				

APPENDIX 4- RISK ASSESSMENT REPORT FOR INDIVIDUAL CLIENTS

CLIENT NAME:				
Risk Parameter	**Description**	**Description**	**Weight (1 to 3)**	**Comments**
Country of birth and residency (low-risk countries?)		If the answer is Yes, the score will be 0		
If answer to above is no, where is the customer born and resides?		If it is a jurisdiction that is sanctioned, the risk will be 3. If it is a jurisdiction that is not sanctioned but deemed high risk, the risk will be 2. Otherwise, it will be 0.		
Presence of PEP		If the individual is a PEP, the score will be 3.		
Sanctions		If the individual is involved with sanctions, the score will be 3.		
Negative information/Red flags from Sum & Substance		If yes, Compliance Team to include in comments		
SUMMARY:				