AML/CFT MANUAL

Version Nº 1.0 |

Date: August 2023 |

Approval by Senior Management	
Date of Last Revision:	
Approval Date:	
Signature of the Senior Management Official:	
Name of the Senior Management Official	
Title of Senior Management Official:	

B2B PRIME SERVICES
AML/CFT MANUAL

Contents

1. DEFINITIONS 5

2. Overview of the Business 6

3. AML/CFT PROGRAM FRAMEWORK 7

3.1. AML/CFT Obligations 7
3.2. Applicable Laws 8
Offence of Money Laundering in accordance with the AML Act (Sec.3) 9
3.3. Anti-money laundering requirements and obligations: 10
3.3.1. The obligations of the Companies include the following: 10
3.3.2. Responsibilities of the Board of Directors 12
3.3.3. Compliance Officer 13
3.3.4. Compliance Officer's Annual Report 15
3.4. B2B's risk-based approach in AML/CFT program development 16
3.4.1. Risk Management 16
3.4.2. Identification of risk 17
3.4.3. Assessment of risk 18
3.4.4. Treatment of risk 23
3.4.5. Monitor and review 24

4. CUSTOMER IDENTIFICATION PROCEDURES 25

4.1. B2B's Customer Due Diligence (CDD) Requirements 25
4.2. Collecting and verifying customer identification information 26
4.3. Identifying and verifying the beneficial owner of a customer 32
4.4. Document Verification Service - individual customer and beneficial owner identification 34
4.5. Record-keeping obligations 34
4.6. Politically exposed persons (PEPs) 34
4.7. Professional Intermediaries and Brokers 35
4.8. Ongoing transaction monitoring 36

5. SUSPICIOUS TRANSACTION REPORTS (STRS) 37

5.1. Submission of information to the FIU 38

6. Tipping Off 39

7. Malice Reporting 40

8. Compliance function in AML and CFT 40

8.1. Responsibilities of AML and CFT Compliance Officer(s) 40
8.2. KNOW YOUR EMPLOYEE 41
8.3. ML and CFT Training Program 42

8.4. Screening Procedures of Personnel Recruitment 43
9. Confidentiality, Security and Protection. 43
10. Period/Frequency of Review of the Manual 43

1. DEFINITIONS

For the purposes of this Manual, unless the context shall prescribe otherwise:

"Anti-Money Laundering" shall mean the actions taken by the Company to prevent, detect and combat money laundering and financing of terrorism activities;

"**AML/CFT**" means Anti-Money Laundering and Countering of Financing of Terrorism

"**Beneficial Owner**" means one or more natural persons who ultimately own or control a customer or the natural person or persons on whose behalf a transaction is being conducted and includes those natural persons who exercise ultimate effective control over a legal person or a legal arrangement;

"**Business Relationship**" means the arrangement between a person and a reporting entity whose primary purpose is to facilitate an occasional or regular course of business dealings between them;

"**Company**" means B2B Prime Servcies SC Ltd which is formed and registered in the Republic of Seychelles under the Companies Ordinance 1972;

"**Compliance Officer**" means the Compliance Officer appointed and approved by the Financial Services Authority of Seychelles, per section 23 (2) of the Financial Services Authority Act 2013 (as amended) and section 34 the Ant-Money Laundering and Countering the Financing of Terrorism Act 2020 (as amended);

"**Customer**" in relation to a transaction or an account, includes—

a) the person in whose name a transaction or account is arranged, opened or undertaken;
b) a signatory to a transaction or account;
c) any person to whom a transaction has been assigned or transferred;
d) any person who is authorised to conduct a transaction; or
e) such other person as may be prescribed by regulations;

"**Data**" means representations in any form of information or concepts;

"**FATF**" shall mean the Financial Action Task-Force;

"**FIU**" means the Financial Intelligence Unit;
"**Law**" shall mean the;

i. Securities Act 2007 (as amended) and the relevant Regulations;
ii. Beneficial Ownership Act 2020 (as amended) and relevant Regulations and guidelines;
iii. Ant-Money Laundering and Countering the Financing of Terrorism Act 2020 (as amended);
iv. FIU Anti-Money Laundering Guidelines; and
v. Any other applicable laws, regulations, codes and guidelines.

"**Money Laundering**" as defined by Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities in Seychelles, is a process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities.

"**ML**" means Money Laundering;

"**Politically Exposed Person (PEP)**" means persons holding prominent public positions in Seychelles or a foreign country such as heads of state or government, senior politicians on the national level, senior government, judicial, military or party officials on the national level, or senior executives of State-owned enterprises of national importance, or individuals or undertakings identified as having immediate or close family ties or personal or business connections to the aforementioned persons;

"**Property**" means currency and assets of any kind, whether corporeal or incorporeal, movable or immovable and legal documents or instruments in any form including electronic or digital, evidencing title to or interest in such assets, including but not limited to bank credits, travelers' cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, whether situated in Seychelles or elsewhere and includes any legal or equitable interest in any such property;

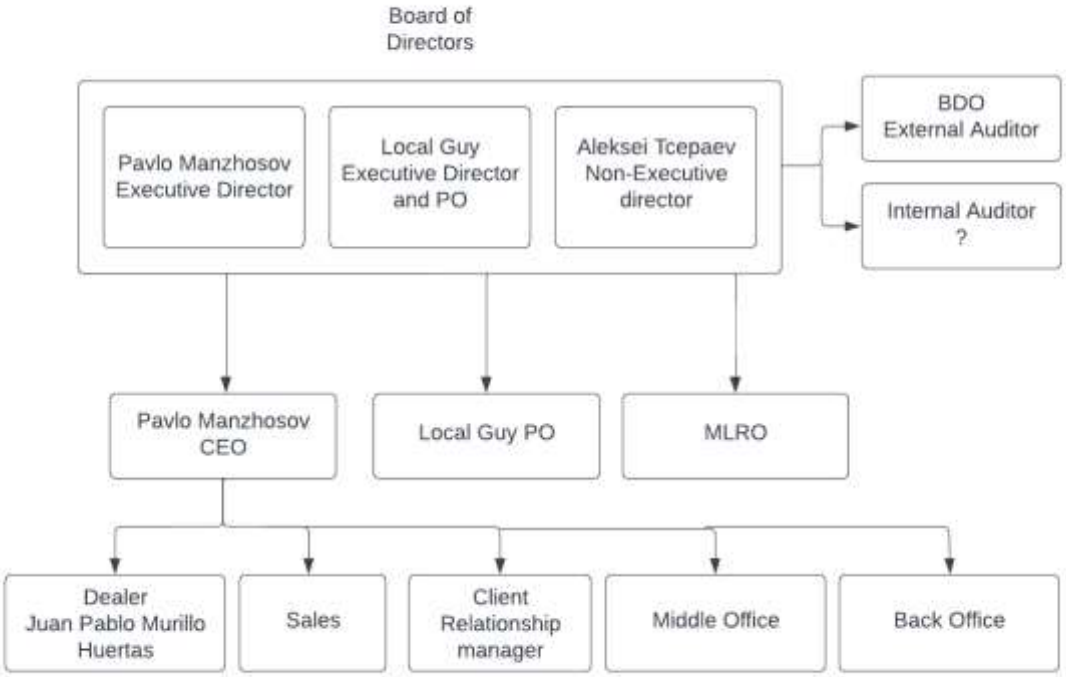
"**STR**" shall mean Suspicious Transaction Report as per section 48 of the Ant-Money Laundering and Countering the Financing of Terrorism Act 2020;

2. Overview of the Business

B2B Prime Services SC Ltd (the "Company") is registered in Seychelles under the Companies Act 1972, with registration number 8435528-1 and licensed as Securities Dealer with the Seychelles FSA with License No.[ ]. The Company's registered address is located at Suite 3, Global Village, Jivan's Complex, Mount Fleuri, Mahe, Seychelles.

The Company will act as a broker providing brokerage services in relation to financial instruments. The Company will principally offer margin trading in rolling spot foreign exchange ("Forex") and CFDs. The Company's income is derived from trading commissions, swap positions and interest earned on overnight positions.

Company Structure



3. AML/CFT PROGRAM FRAMEWORK

3.1. AML/CFT Obligations

We pledge to diligently adhere to international anti-money laundering and counter-terrorist financing standards, including the guidelines set forth by regulatory authorities. Our dedication extends to the continuous enhancement of policies, procedures, and controls to identify and mitigate ML/TF risks effectively. We recognize our role as a reporting entity in safeguarding the integrity of the financial system and pledge to cooperate fully with relevant authorities, employing a proactive approach to

combat illicit financial activities and ensure compliance with all applicable laws and regulations.

B2B Prime Servcies SC Ltd (the “Company” or “B2B”) has in place an AML/CFT Program that covers the Company’s customer due diligence (CDD) procedures including:

a. establishing a framework for identifying customers and beneficial owners of customers so the Company can be reasonably satisfied a customer is who they claim to be;
b. collecting and verifying customer and beneficial owner information; and
c. monitoring customers transaction and ensuring that information in records are always relevant and updated.

B2B's Compliance Officer will conduct regular AML/CFT reviews to ensure B2B is in compliance with the AML/CFT Rules and with its AML/CFT Program. To the extent necessary, the Compliance Officer will also arrange for periodic independent external reviews in accordance with the requirements of the AML/CFT Act.

The primary purpose of the program is to make sure that business of B2B is conducted in compliance with international AML/ CFT rules and Financial Action Task Force’s recommendation. B2B has established a framework and has documented its customer due diligence (CDD) procedures in detail in this document which will help B2B identify its customers and understand its customers' financial activities.

Identification and verification of customer’s identity will effectively mitigate B2B’s ML/TF risks in the conduct of financial transactions, particularly where the activity or transactions are unusual or uncharacteristic.

This policy is made available to all the Company’s employees especially the Customer Service officers as they are B2B’s first line of defense against ML/TF; the department primarily carries out client onboarding, maintenance of client’s relationship and review client’s fund withdrawal request. Upon reading and understanding the manual, each employee shall be required to acknowledge their comprehension and commitment to adhere to its provisions by signing an acknowledgment form (Appendix A) provided with this manual. All staffs have been cautioned of the impact in the event of non-adherence to the policy. Furthermore, AML/CFT training is administered to all personnels on periodic basis to ensure that employees are always kept up to date to AML/CFT development.

3.2. Applicable Laws

The relevant regulatory requirements that the Company must comply with are as follows:

- AML and CFT Act, 2020 and its subsequent amendments
- AML and CFT Regulations, 2020
- Companies Ordinance, 1972
- Beneficial Ownership Act, 2020
- Beneficial Ownership Regulations, 2020
- Prevention of Terrorism Act, 2004 (and subsequent amendments)
- Prevention of Terrorism Regulations, 2015
- Securities Act, 2006 and its subsequent amendments
- Securities Conduct of Business Regulations 2008
- Financial Consumer Protection Act 2022

Additional guidance for interpretation and good practices that B2B may refer to includes:

- Guidance on Transparency and Beneficial Ownership issued by the FATF in October 2014
- Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities in Seychelles (updated) in June 2015.
- Beneficial Ownership Guidelines

Offence of Money Laundering in accordance with the AML Act (Sec.3)

The AML Act (Sec.3) extensively defines the offence of money laundering 3(1):

1. A person is guilty of money laundering if, knowing or believing that property is or represents the benefit of criminal conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse (the proof of which shall lie on the person) —
    a) converts, transfers or handles the property, or removes it from the Republic;
    b) conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it; or
    c) acquires, possesses or uses the property.

2. Removing property from the Republic shall include references to removing it from another country or territory and moving property within the Republic or a country or territory in preparation for or for the purpose of removing it from the Republic or the country or territory in question.

3. Any person who participates in such conduct as described in subsections (1)(a), (1)(b) or (1)(c) of this section including but not limited to, aiding, abetting, assisting, attempting, counselling, conspiring, concealing or procuring the commission of such conduct commits the offence of money laundering as a principal offender and shall be liable to be tried and punished.

4. A) a person guilty of money laundering is liable on conviction to a fine not exceeding SCR5,000,000 or to imprisonment for a term not exceeding 15 years or to both;
    B) a person other than a natural person guilty of money laundering is liable on conviction to a fine not exceeding SCR10,000,000.

5. Where a person —

(a) converts, transfers, handles or removes from the Republic any property which is or represents the benefit from criminal conduct;
(b) conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it; or
(c) acquires, possesses or uses the property, in such circumstances that it is reasonable to conclude that the person —

(i) knew or believed that the property was or represented benefit of criminal conduct, or
(ii) was reckless as to whether it was or represented benefit from criminal conduct, that person shall be taken to have so known or believed or to have been so reckless, unless the court is satisfied having regard to all the evidence that there is a reasonable doubt as to whether the person so knew or believed or was so reckless.

3.3. Anti-money laundering requirements and obligations:

There are five key anti-money laundering requirements that are specific to "regulated activity". These provides a useful approach for the Company to consider when looking at how to manage the money laundering risk.

- ✓ Customer identification procedures,
- ✓ Record keeping procedures in relation to customer's identity and their transactions,
- ✓ Procedures of internal reporting to the Compliance and CO appointed to receive and consider information that give rise to knowledge or suspicion that a customer is engagedin money laundering activities,
- ✓ Other internal control and communication procedures for the purpose of forestalling andpreventing money laundering,
- ✓ Measures for making employees aware of the above procedures to prevent money laundering and of the legislation relating to money laundering; and Provision of training to their employees in the recognition and handling of transactions suspected to be associated with money laundering and suspicious transactions.

3.3.1. The obligations of the Companies include the following:

The Company shall establish and maintain procedures and systems to:

a) implement internal policies, procedures and controls to fulfil the obligations

under this Act;

b) implement adequate screening procedures to screen persons before recruitment;

c) train its officers, employees and agents to recognise suspicious transactions, trends in money laundering, and terrorist financing activities and risks within the Company' products, services and operations; and

d) implement independent audit arrangements to test its procedures and systems relating to anti-money laundering, and terrorist financing activities.

e) The need to identify and verify the identity of a customer when establishing a business relationship; If the customer is a politically exposed person ("PEP"), a Company shall adequately identify the person and verify his or her identity. In addition, to have appropriate risk management systems to determine whether the customer is a PEP.

f) To apply enhance customer due diligence measures and enhanced ongoing monitoring for PEP.

g) Take reasonable measures to ascertain the purpose of any transaction in excess or equivalent to SCR 50,000 (or equivalent in another currency) or in excess or equivalent of SCR 50,000 (or equivalent in another currency) in the case of cash transactions, and the origin and ultimate destination of the funds involved in the transaction.

h) To retain the details and report to the FIU the particulars concerning cash transactions of SCR50,000 or more or the equivalent money in the currency of other countries or wire transfer that is executed of SCR 50,000 or more of the equivalent money in the currency of other countries.

i) In relation to its cross–border banking and other similar relationships adequately identify the identity of the person, gather sufficient information about the nature of the business, assess the AML/CFT controls and obtain senior management's permission before entering into a new relationship;

j) Identify and assess money laundering and terrorist financing risks

k) To not proceed with a transaction if there is no satisfactory evidence of a customer's identity;

l) To maintain records on a customer's identity for a minimum period of 7 years from the date of any transaction or correspondence or on which the business relationship ceases; A Company that fails to maintain records is guilty of an offence.

m) Maintain accounts in their true name;

n) Ensure that money transmission includes accurate originator information on electronic funds transfers and that the information shall remain with the transfer;

o) To monitor complex, unusual or large transactions with no apparent economic or lawful purpose as well as ongoing monitoring of business relationships /transactions undertaken throughout the course of the relationship;

p) To report any transaction or attempted transaction that may be related to the commission of an offence of ML/FT to the FIU within two business days of forming the suspicion or receiving the information.

q) Further to the abovementioned obligations, reporting entities should therefore ensure that their staff are fully aware of their obligations found in the law and abide by them so as to ensure compliance. Therefore, a Company shall Company's compliance with the provisions of this Act.

r) The Company, if required must also appoint an alternate Compliance Officer who will be acting in the absence of the Compliance Officer. The individual appointed as Alternate Compliance Officer will undergo a fit and proper assessment by the FSA for approval.

3.3.2. Responsibilities of the Board of Directors

The responsibilities of the Board in relation to the prevention of money laundering and terrorist financing include the following:

- Obligation to identify and assess money laundering and terrorist financing risks
- Obligation to establish and maintain internal control systems and procedures
- to determine, record and approve the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing and communicate them to the CO.
- to appoint the CO and, where is necessary, assistant COs and determine their duties and responsibilities, which are recorded in this Manual
- to approve the Manual
- to ensure that all requirements of the Law and of the Directive are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement
- to assure that the CO and his assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all data and information concerning Clients' identity, transactions' documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as included herein

- to ensure that all employees are aware of the person who has been assigned the duties of the CO, as well as his assistants (if any), to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing

- to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the CO, either directly or through his assistants, if any, and notifies accordingly the CO for its explicit prescription in the Manual

- to ensure that the CO has sufficient resources, including competent staff and technological equipments, for the effective discharge of his duties

- to assess and approve the CO's Annual Report and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report

- to approve the mandatory annual training program prepared by the CO, ensuring to receive adequate management information on the implementation of the Company's AML/CFT training program and ensure to be adequately trained to be well aware and up to date with the regulatory framework and the relevant responsibilities deriving from this.

3.3.3. Compliance Officer

The CO shall belong hierarchically to the higher ranks of the Company's organizational structure so as to command the necessary authority. The CO shall lead the Company's AML/CFT compliance procedures and processes and report to the Board. The CO shall at all times be resident in Seychelles. In addition, an alternate to the CO be appointed to assume the prescribed responsibilities and duties in the CO`s absence.
As per section 34 of the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020, the Company shall within 30 days of the commencement of its operations:

a) appoint the Compliance Officer who shall be responsible, for ensuring the compliance with the provisions of AML and CFT Act, 2020, with the approval of the respective supervisory authority:

b) the CO appointed pursuant to this section will:

I. be a senior officer with the necessary qualifications and experience and able to respond adequately to enquiries relating to the Company and the conduct of its business;
II. be a resident in Seychelles;
III. be responsible for the implementation and on-going compliance of the company's internal programs, controls and procedures in relation to its business with the requirements of AML and CFT Act, 2020;
IV. be responsible for ensuring that Company's staff comply with the provisions of the AML and CFT Act, 2020 and any other law relating to ML or TF and the provisions of any manual of compliance procedures established; and
V. act as the liaison officer between the company and the supervising authority and

the FIU in matters relating to compliance with the provisions the AML and CFT Act, 2020 and any other law with respect to ML or TF;

VI. be familiar with the provisions of the guidelines that may be issued by the FIU and the relevant supervisory authority;

VII. have unrestricted access on demand to all books, records and employees of the company as may be necessary to fulfil his or her responsibilities;

VIII. receive and review reports of suspicious transactions, or suspicious activities made by the staff of the company and, if sufficient basis exists, report the same to the FIU in accordance with the AML and CFT Act, 2020; and

IX. implement record keeping and retention requirements under sections 47 of the AML and CFT Act, 2020;

X. implement the reporting requirements under section 48 of the AML and CFT Act, 2020, with regard reporting suspicious transaction or certain information;

XI. ensure the Company's officers and employees are aware of the laws and Regulations relating to ML and TF;

XII. ensure the Company's officers, employees and agents recognize suspicious transactions, trends in ML and TF activities and ML and TF risks within the Company's products, services and operations.

XIII. To develop a compliance culture —

a) to ensure that all directors and relevant staff are familiar with the laws and regulations of the Seychelles to combat money laundering and terrorist financing activities, which includes an understanding of the relevant compliance policies, procedures and systems of the company as well as, the compliance officer imparts awareness of the need for compliance, thereby, developing within the company a robust compliance culture;

b) to monitor the developments and changes in the legislation, policies, standards and other guidelines issued by the international bodies in order to keep the company updated with the regulatory developments and changes in international requirements;

XIV. to implement the training program —

a) for directors and relevant staff which includes the training program on general Anti-Money laundering and countering the financing of terrorism awareness, client acceptance procedures, know your customer (KYC) procedures, remediation and suspicious activity reporting relevant to the company's activities;
b) at least once in every year and whenever there are changes in the laws, regulations or international requirements to ensure that the directors and related staff are aware of the latest developments in the Anti-Money laundering and countering the financing of terrorism activities;
c) to undergo additional training, in order to enhance his or her professional skills, at least once every year;

XV. to perform review of the compliance framework and make regular assessment reports to the senior management, identify the deficiencies and making recommendations for any updates or revisions;

XVI. to ensure the preparation and submission of an annual compliance report to the supervisory authority for information within 90 days after each calendar year.

XVII.

3.3.4. Compliance Officer's Annual Report

The Annual Report of the CO or alternate CO is a significant tool for assessing the Company's level of compliance with its obligation laid down in the Laws and Regulations.
This Annual Report shall be prepared and be submitted to the Board for approval within two (2) months from the end of each calendar year (i.e., the latest, by the last day of the month of February of each calendar year). Following the Board's approval of the Annual Report, a copy of this Annual Report shall be submitted to the FSA together with the Annual AML/CFT Compliance Form and Business Risk Assessment . It is provided that minutes shall include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures.

The Annual Report deals with issues relating to ML and TF during the year under review and includes, inter alia, the following:

a) information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and Regulations which took place during the year under review;
b) information on the inspections and reviews performed by the CO or alternate to the CO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of ML and TF. In this respect, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation;
c) the number of internal STRs submitted by Company personnel to the CO or alternate to the CO, and possible comments/observations thereon;
d) the number of STRs submitted by the CO or alternate to the CO to the FIU, with information/details on the main reasons for suspicion and highlights of any particular trends;
e) information, details or observations regarding the communication with the employees on ML and TF preventive issues;
f) information on the policy, measures, practices, procedures and controls applied by the Company in relation to high-risk customers as well as the number and country of origin of high-risk customers with whom a business relationship is established or a one-off transaction has been executed;
g) information on the systems and procedures applied by the Company for the ongoing monitoring of customer accounts and transactions, as and when applicable;
h) information on the training courses/seminars attended by the CO or alternate to the CO and any other educational material received;
i) information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organized, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants;
j) results of the assessment of the adequacy and effectiveness of staff training;
k) information on the recommended next year's training program;
l) information on the structure and staffing of the department of the CO or alternate to the CO, as well as, recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against ML and TF; and

m) an executive summary in respect to the key findings and weaknesses identified during the year under review.

3.4. B2B's risk-based approach in AML/CFT program development

B2B use a risk-based approach in developing its AML/CFT program and within this approach it identifies and assess the risks its business faces according to the types of customers it serves, the products and services it provides to customers, the delivery channel, and the jurisdiction in consideration. After the risk analysis and categorization, B2B will develop controls, procedures and allocate resources that are proportionate to those risks.

In a risk-based approach model, B2B will allocate additional efforts to those areas of the business it assesses as having a higher ML/TF risk (if any). This gives B2B a degree of flexibility to determine how its obligations can be implemented and enables B2B to tailor its AML/CFT program to meet the specific features, risks and characteristics of the business.

3.4.1. Risk Management

The risk management table as seen shows the steps that B2B will undertake to identify, categorize and address the ML/TF risk it faces.

Step	**Description**
Risk identification	**Identify the main ML/TF risks:** customers products & services business practices/delivery methods countries you do business with **Identify the main regulatory risks**.

Risk assessment/measurement	**Measure the size & importance of risk:** likelihood - chance of the risk happening impact - the amount of loss or damage if the risk happened likelihood X impact = level of risk (risk score)
Risk treatment	**Manage the business risks:** minimise and manage the risks apply strategies, policies and procedures **Manage the regulatory risks:** put in place systems and controls carry out the risk plan & AML/CFT program
Risk monitoring and review	**Monitor and review the risk plan:** develop and carry out monitoring process keep necessary records review risk plan and AML/CFT program do internal audit or assessment do AML/CFT compliance report

3.4.2. Identification of risk

Customers (examples):

a. The customer identity, origin of wealth or source of funds cannot be easily verified;
b. Where the structure of the customer/entity renders it difficult to identify the true controlling owner, or where there is no legitimate commercial rationale for the structure;
c. The customer is a Politically Exposed Persons ("PEP");
d. Customers who appear on governments lists, including sanction lists, or other credible sources which trigger risks in respect of corruption and/or criminal activity;
e. Customers (not necessarily PEPs) based in, or conducting business in or a high-risk geographic location, or a geographic location with known higher levels of corruption or organized crime, or drug production/distribution;
f. Charities and other "not for profit" organizations which are not subject to some form of regulatory monitoring or supervision;
g. Professional service providers such as lawyers, accountants, investment brokers or other

professionals holding accounts for their customers or acting on behalf of their customer and where we would be required to place an unreasonable reliance on the professional service provider;

h. Requests for undue levels of secrecy with a transaction;
i. Whether the customer is a long-standing customer or undertakes occasional transactions;

the customer's business activities place the customer in a high-risk category (military, casino).

Products and services (examples):

a. Services where large amounts are invested;
b. Services involving structures intended to (or which can in practice) render a customer anonymous (e.g., accounts in the names of trusts or nominees of third persons);
c. Services whereas the client trades for no apparent speculation, arbitrage or hedging purpose.
d. Services where the client intends to trade at conditions (e.g., fees) that are clearly unfavorable to him/her.

Business practice/delivery method (channels):

a. Non face to face
b. Through third-party agent or broker.

Country/jurisdiction:

a. Countries identified by credible sources as providing funding or support for terrorist activities or who have terrorist groups working within the country;
b. Countries subject to sanctions and embargoes by the United Nations;
c. Countries identified by credible sources as having significant levels of corruption and/or criminal activity;
d. Countries identified by credible sources as lacking appropriate AML and CFT legislation;
e. Countries identified by the FATF as non-co-operative countries and territories.

Regulatory risk

This risk is associated with not meeting the requirements of the AML/CFT Act. Examples of some of these risks are:

a. customer verification not done properly
b. failure to train staff adequately
c. not having an AML/CFT program
d. failure to report suspicious matters
e. not having an AML/CFT Compliance Officer.

3.4.3. Assessment of risk

After identification of risk, the next step is to assess the risk based on the likelihood that such a risk will

occur and the impact if it occurs.

Table 1: Risk management worksheet - risk

Risk group:	**Customers**			
Risk	Likelihood	Impact	Risk score	Treatment/ Action
New customer *(example only)*	-	-	-	-
Customer who brings in large amounts of used notes and/or small denominations *(example only)*	-	-	-	-
Customer whose business is registered overseas with no Australian office *(example-only)*		-	-	-

Measure the size & importance of risk:

- likelihood - chance of the risk happening
- impact - the amount of loss or damage if the risk happened
- likelihood X impact = level of risk (risk score)

Having identified the risks involved, they need to be assessed or measured in terms of the chance (likelihood) they will occur and the severity or amount of loss or damage (impact) which may result if they do occur. The risk associated with an event is a combination of the chance (likelihood) that the event will occur and the seriousness of the damage (impact) it may do.

Therefore each risk element can be rated by:

- the chance of the risk happening - 'likelihood'
- the amount of loss or damage if the risk happened - 'impact' (consequence).

To help assess the risks identified in the first stage of this process, we can apply the risk rating scales for likelihood (*Table 2*) and impact (*Table 3*) and from these get a level of risk or risk score using the risk matrix below.

Likelihood x Impact = Risk level/Score

Likelihood scale

A likelihood scale refers to the potential of an ML/TF risk occurring in our business for the particular risk being assessed. Three levels of risk are shown in Table 2, but you can have as many as you believe are necessary.

Table 2: Likelihood scale

Frequency	**Likelihood of an ML/TF risk**
Very likely	Almost certain: it will probably occur several times a year
Likely	High probability it will happen once a year
Unlikely	Unlikely, but not impossible

Impact scale

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen.

In assessing the possible impact or consequences, the assessment can be made from several viewpoints. Following is a list of ideas. It does not cover everything and it is not prescriptive.

Impact of an ML/TF risk could, depending on circumstances, be rated or looked at from the point of view of:

a. how it may affect our business if, through not dealing with risks properly, we suffer a financial loss from either a crime or through fines from the regulator
b. the risk that a particular transaction may result in the loss of life or property through a terrorist act
c. the risk that a particular transaction may result in funds being used for any of the following: corruption, bribery, smuggling of goods/workers/immigrants, banking offences, narcotics offences, psychotropic substance offences, slavery and trade in women and children, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud
d. the risk that a particular transaction may cause suffering due to the financing of illegal drugs
e. reputational risk - how it may affect our business if we are found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being shunned by your own

community of customers

f. how it may affect your wider community if you are found to have aided an illegal act; the community may get a bad reputation as well as your business.

Three levels of risk are shown in Table 3 (but we can have as many as we believe are necessary).

Table 3: Impact scale

Consequence	**Impact - of an ML/TF risk**
Major	Huge consequences - major damage or effect. Serious terrorist act or large-scale money laundering.
Moderate	Moderate level of money laundering or terrorism financing impact.
Minor	Minor or negligible consequences or effects.

Risk matrix and risk score

Use the risk matrix to combine LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk. How the risk score is derived can be seen from the risk matrix and risk score table (*Table 4*) shown below. Four levels of risk or score are shown in the matrix and Table 4 (but we can have as many as you believe are necessary).

Matrix: Threat level for ML/TF risk

Likelihood	**Impact - how serious is the risk?**		
Very likely	Medium 2	High 3	Extreme 4
Likely	Low 1	Medium 2	High 3

Unlikely	Low 1	Low 1	Medium 2
What is the chance it will happen?	**Minor**	**Moderate**	**Major**

Table 4. Risk score table

Rating	**Impact - of an ML/TF risk**
4 Extreme	**Risk almost sure to happen and/or to have very dire consequences.** **Response:** **Do not allow transaction to occur or reduce the risk to acceptable level.**
3 High	**Risk likely to happen and/or to have serious consequences.** **Response:** **Do not allow transaction until risk reduced.**
2 Medium	**Possible this could happen and/or have moderate consequences.** **Response:** **May go ahead but preferably reduce risk.**
1 Low	**Unlikely to happen and/or have minor or negligible consequences.** **Response:** **Okay to go ahead.**

Once threat levels and risk scores have been allocated, they can be entered in the risk management worksheet (*Table 5*) next to the risk.

Table 5: Risk management worksheet - threat level and risk score

Risk group:	**Customers**			
Risk	Likelihood	Impact	Risk score	Treatment/Action
New customer *(example only)*	Likely (*example only*)	Moderate (*example only*)	2 (*example only*)	
Customer who brings in large amounts of used notes and/or small denominations *(example only)*	Likely (*example only*)	Major (*example only*)	3 (*example only*)	

Customer whose business is registered overseas with no Australian office *(example only)*	Very likely (*example only*)	Major (*example only*)	5 (*example only*)
Customer whose business is registered overseas with no Australian office (example only)	Very likely (example only)	Minor (example only)	2 (example only)

3.4.4. Treatment of risk

Using the matrix above, all customers will be assigned risk level of 1-4. the Company will devise measures to minimize and manage the risks example applying enhanced due diligence to high-risk customers. Monitoring of customers' activities and transactions will be carried out manually by Customer Service department whereas senior management and compliance manager will have oversight electronically.

If need be, the Company will also increase the frequency of staff training so to effectively increase staff awareness and knowledge of AML and CFT, mitigating risk of B2B in breaching AML/CFT business and regulatory risk.

Examples of a risk reduction or treatment step are:

a. setting transaction limits for high-risk customers
b. having a management approval process for higher-risk customers
c. process to place customers in different risk categories and apply different identification and verification methods
d. not accepting an overseas customer where the impact is high.

You could record this using *Table 6*.

Table 6: Risk management worksheet - risk treatment or action

Risk group:	**Customers**			
Risk	Likelihood	Impact	Risk score	Treatment/Action

New customer *(example only)*	Likely (*example only*)	Moderate (*example only*	2 (*example only*)	Standard ID check ID verification type X
Customer who brings in large amounts of used notes and/or small denominations *(example only)*	Likely (*example only*)	Major (*example only*)	3 (*example only*)	Non-standard ID check ID verification type X
Customer whose business is registered overseas with no Australian office *(example only)*	Very likely (*example only*)	Major (*example only*)	5 (*example only*)	Do not accept as customer
Customer whose business is registered overseas with no Australian office (example only)	Very likely (example only)	Minor (example only)	2 (example only)	Standard ID check + ID verification type Additional Info

Another way to reduce the risk is to use a combination of risk groups to modify the overall risk of a transaction. B2B may approve a combination of your customer, product/service and country risk with a modified overall risk.

For example, in the case of fund remittance, for a low-risk customer we may decide to only use a bank account-to-bank account service (assessed as low risk by you) to a certain city/province (assessed as a high risk area by you) in a certain country (assessed as low risk by you).

Or in the case of onboarding an overseas company, we shall generally classify them as at least medium risk and only accept them as a client if the impact as assessed by us is minor, for example due to the client being (managed by) a licensed financial services provider in an acceptable jurisdiction (such as Guernsey) and therefore being subject to appropriate rules and regulations (including KYC AML/CFT Rules).

It is important to remember that identifying, for example, a customer, transaction or country as high risk does not necessarily mean that money laundering or terrorism financing is involved. The opposite is also true: just because a customer or transaction is seen as low risk does not mean the customer or transaction in not involved in money laundering or terrorism financing. Experience and common sense will be applied to the risk management process.

3.4.5. Monitor and review

Keeping records and regular evaluation of your risk plan and AML/CFT program is essential. The risk

management plan and AML/CFT program will be reviewed on annual basis or as risks change over time by the Compliance Manager who may seek external compliance auditor help. Examples of risk change will be changes to customer base, products and services, business practices and the law.

The annual review will document whether the AML/CFT program is working correctly and well. If not, the Compliance Manager with support from senior management will work out what needs to be improved and put changes in place. This will help keep your program effective and also meet the requirements of the AML/CFT Act.

4. CUSTOMER IDENTIFICATION PROCEDURES

4.1. B2B's Customer Due Diligence (CDD) Requirements

B2B's CDD requirements include:

a. collecting and verifying customer identification information - for example, documents, data or other information obtained from a reliable and independent source;
b. identifying and verifying the beneficial owner(s) of a customer;
c. identifying whether a customer is a PEP (or an associate of a PEP) or is there negative news in relation to customer and taking steps to establish the source of funds used during the business relationship or transaction;
d. ongoing customer due diligence and transaction monitoring; and
e. obtaining information on the purpose and intended nature of the business relationship.

When does Anchor need to undertake CDD?

Except in special circumstances or if an exemption applies, the CDD obligations must be completed before the provision of the designated service, regardless of whether it involves a one-off transaction or an ongoing business relationship.

B2B will identify the beneficial owner of a customer and determine whether the customer or a beneficial owner is a PEP, passed negative news screening before it provides the designated service.

Risk-based customer due diligence procedures

B2B established and put into practice a risk-based CDD procedures. In the development of these procedures, B2B considers the risk posed by each of the following factors:

a. customer types, including beneficial owners of customers, PEPs and negative news alert
b. customers' sources of funds and wealth (for example, by enquiring into the expected source and origin of the funds to be used in the provision of the designated service)
c. nature and purpose of the business relationship (for example, the customer's business or employment or whether the customer is a licensed financial services company itself)
d. control structure of non-individual customers (for example, complex corporate structures and the underlying beneficial owners)
e. how B2B provides its designated services (for example, online)
f. foreign jurisdictions in which B2B deals (for example, customers that live or are incorporated in a foreign country).

4.2. Collecting and verifying customer identification information

What are the minimum customer identification and verification requirements?

Individual customer

Name and date of birth (DOB)

Collect and verify the full name and the date and place of birth of the individual either from the ID or passport of the person.

Address

Collect the proof of residential address not older than 3 months such as:

i. Utility bill,
ii. Bank Statements,
iii. Phone bill

(this list is not exhaustive)

PEPs

Determine whether the individual is a PEP

Beneficial owner(s)

For individuals, a reporting entity may assume that the customer and beneficial owner are the same person, unless there are reasonable grounds to consider otherwise

Company & Sole Proprietorship

Name

Collect and verify the full name of the company

Address

Collect the full address of the principal place of business of the company in the country of formation or incorporation

Other

Collect the country in which the company was formed or incorporated

Beneficial owner(s)

Identify the beneficial owner(s) of the company

Determine whether each beneficial owner of the company is a PEP

Identification and verification of the beneficial owner(s) is not required for a foreign listed public company which is subject to 'transparency of beneficial owner' disclosure requirements

The following documents shall be collected:

i. Certificate of incorporation
ii. Memorandum & Articles
iii. Registers of Directors & Shareholder
iv. Certificate of good standing (if any)
v. Bank statement not older than 6 months or the financial statement not older than 1 year
vi. The proof of address and identification of:
    - The Director(s)
    - Shareholder(s)
    - Beneficial Owner(s)

Simplified company verification procedure

Confirm that the company is either:

a listed public company licensed entity

Identification and verification of the beneficial owner(s) is not required for a company which has been verified under the 'simplified company verification procedure'.

Partnership

Name

Collect and verify the full name of the partnership

Collect the full business name as registered with any state or territory business name authority

Collect the full name of each partner (not required if the regulated status of the partnership is confirmed

by referring to a current membership directory of the relevant professional association)

Address

Collect the full residential address of each partner (not required if the regulated status of the partnership is confirmed by referring to a current membership directory of the relevant professional association)

Other

Collect the name of the country in which the partnership was established

Collect and verify the information relating to one of the partners (as per the 'Individual' identification procedure)

Beneficial owner(s)

Identify the beneficial owner(s) of each partner

Determine whether each of the partners or the beneficial owner of each partner is a PEP

Trustee

It is mandatory to collect the Trust Deed for conducting due diligence.

Name

Collect and verify the full name of the trust

Collect the full business name (if any) of the trustee of the trust

Collect the full name of all trustees

Collect and verify the settlor of the trust, unless:

- the material asset contribution to the trust by the settlor at the time the trust is established is less than $10,000; or
- the settlor is deceased; or
- the trust is verified using the simplified trustee verification procedure

Address

Collect the full address of all trustees

Other

Collect information regarding the type of trust and the country in which the trust was established

Beneficiaries

Collect **one** of the following:

- full name of each beneficiary of the trust
- if beneficiaries are identified by reference to a class, details of the class

Sole trustee

Collect and verify information relating to the sole trustee (as per appropriate 'Individual' or 'Company' identification procedure)

Multiple trustees

Collect and verify information relating to one trustee (as per appropriate 'Individual' or 'Company' identification procedure)

Beneficial owner(s)

Identify the beneficial owner(s) of the trust

Determine whether each beneficial owner of the trust is a PEP

Simplified trustee verification procedure

Confirm that the trust is either:

registered and subject to regulatory oversight in relation to its trust activities

a government superannuation fund established by legislation

Association

Name

Collect and verify the full name of the association

Collect the full name of the chairman, secretary and treasurer or equivalent officer (in each case)

Address

Collect **one** of the following:

Full address of the principal place of administration or registered office (if any) (only **one** of these required for collection)

Residential address of the public officer

Residential address of the president, secretary or treasurer (if no public officer) (only **one** of these required for collection)

Other

Collect and verify any unique identifying number issued to the association by the incorporating state, territory or overseas 'incorporation body'

Beneficial owner(s)

Identify the beneficial owner(s) of the association

Determine whether each beneficial owner of the association is a PEP

Unincorporated Association

Name

Collect and verify the full name of the association

Collect the full name of the chairman, secretary and treasurer or equivalent officer (in each case)

Address

Collect the full address of the principal place of administration (if any)

Other

Collect and verify information relating to the member (as per the appropriate 'Individual' identification procedure where the customer is acting in the capacity of a member of the unincorporated association

Beneficial owner(s)

Identify the beneficial owner(s) of the association

Determine whether each beneficial owner of the association is a PEP

Registered co-operative

Name

Collect and verify the full name of the co-operative

Collect the full name of the chairman, secretary and treasurer or equivalent officer (in each case)

Address

Collect only **one** of the following:

Full address of the registered office

Principal place of operations (if any)

Residential address of the co-operative's secretary

Residential address of the co-operative's president or treasurer (if no secretary)

Other

Collect and verify any unique identifying number issued to the co-operative on registration by the state, territory or overseas 'registration body'

Beneficial owner(s)

Identify the beneficial owner(s) of the registered co-operative

Determine whether each beneficial owner of the registered co-operative is a PEP

Government body

Name

Collect and verify the full name of the government body

Address

Collect and verify the full address of the government body's principal place of operations

Other

Collect and verify whether the government body is:
a separate legal entity, agency or authority; and/or
established under legislation of the Commonwealth, state or territory or a foreign country; and if so the name of the state, territory or foreign country

Beneficial owner(s)

Identification and verification of the beneficial owner(s)

Agent Of an individual customer

Name

Collect the full name of each agent acting on the customer's behalf regarding the provision of the designated service(s)

Other

Collect evidence (if any) of the authorization of the agent to act on behalf of the customer

Agent Of a non-individual customer

Name

Collect the full name of each agent acting on the customer's behalf regarding the provision of the designated service(s)

Other

Collect evidence of the authorization of the agent to act on behalf of the customer

Requirements for medium and higher risk customers

For medium risk customers, B2B will require customer identity and verification documentation as seen above and as specified elsewhere in this document and the KYC AML/CFT Compliance Officer will decide on a case-by-case basis what additional information is to be collected and verified (if any).
For higher risk customers, B2B will obtain senior management approval before establishing or

continuing a business relationship with the customer and before providing, or continuing to provide, a designated service to the customer, take reasonable measures to establish the customer's source of wealth and source of funds and comply with enhanced customer due diligence requirements.

4.3. Identifying and verifying the beneficial owner of a customer

B2B implement the following procedures to collect and verify identification information about the beneficial ownership and control of its customers.

What is a beneficial owner?
A beneficial owner of a customer is defined as an individual (a natural person or persons) who ultimately owns or controls (directly or indirectly) the customer.

Ownership for the purposes of determining a beneficial owner means owning 25 per cent or more of the customer.

The definition of 'control' includes whether the control is exerted by means of trusts, agreements, arrangements, understandings or practices and whether or not the individual has control based on legal or equitable rights. It includes where an individual can exercise control through making decisions about financial and operating policies.

What beneficial owner information must be collected and verified?
Once B2B has established who is a beneficial owner or owners of a customer, B2B shall collect at least the following information in relation to each individual beneficial owner:

full name; and
date of birth **or** full residential address.

B2B will take reasonable measures to verify the information it collects about the beneficial owner that is appropriate given the level of ML/TF risk.

How does B2B identify the beneficial owner of a customer?
To identify the beneficial owner of a customer, B2B should establish and understand the ownership or control structure of the customer. In most cases, B2B can request information from the customer. B2B may also need to enquire further into a complex ownership or control structure.

Examples of information that may assist B2B in identifying a beneficial owner of a customer include:

a certificate of incorporation of a company and/or an annual statement
a trust deed
a partnership agreement
the constitution and/or certificate of incorporation for an incorporated association
the constitution of a registered co-operative.

What process should B2B take if it is unable to identify the beneficial owner of a customer?
In some cases, where no person owns 25 per cent or more of the customer or where there is not an individual exercising control of the customer.

In these cases, B2B is required to identify and take reasonable steps to verify an alternative individual as described below:

The customer is a company or a partnership:
B2B will attempt to identify an individual in the following order:

an individual who can exercise 25 per cent or more of the voting rights, including the power to veto. The power to exercise voting rights may be direct or indirect, including where the individual is entrusted with, or has significant influence over, the exercise of the voting rights.

If the reporting entity cannot identify the above individual:

any individual who holds the position of senior managing official (or equivalent).

The customer is a trust:

B2B will attempt to identify any individual who holds the power to appoint or remove the trustees of the trust. This role is usually described as the appointor but may also be called the 'custodian' or 'principal', and should be noted in the trust deed.

The customer is an association or a registered co-operative:

B2B will attempt to identify an individual in the following order:
It should attempt to identify any individual who can exercise 25 per cent or more of the voting rights, including a power to veto.
If the reporting entity cannot identify the above individual, it should attempt to identify any individual who

would be entitled to 25 per cent or more of the property of the association or registered cooperative if it were dissolved.
If the reporting entity cannot identify an individual described in 1 or 2 above, it should attempt to identify any individual who holds the position of senior managing official.

4.4. Document Verification Service - individual customer and beneficial owner identification

B2B uses a third-party identity verification platform to verify customer's identification document received. The platform provides access to more than 450 data sources worldwide allowing verification of more than 5 billion consumers from 195 countries.

With AI-driven insights and real-time analytics, B2B is able to verify the veracity of government issued identity documents and the validity of proof of address allowing B2B to testify that the identity document presented by an individual is current and/or valid.

4.5. Record-keeping obligations

B2B will keep all records of the applicable customer identification procedure (ACIP) they undertake in respect to each customer, and of the information they obtain in the course of carrying out that procedure for a 7-year period which will commence after the ACIP is carried out and last throughout the whole of which B2B did not provide any designated services to the customer.

In addition to ACIP, B2B will also maintain in records the following for a 7-year period;

- transaction records
- electronic funds transfers
- AML/CFT programs
- due diligence assessments of correspondent banking relationships.

4.6. Politically exposed persons (PEPs)

Who is a politically exposed person?

Politically exposed persons (PEPs) are individuals who occupy a prominent public position or function in a government body or international organization. This definition also extends to their immediate family members and close associates.

When does a person cease to be considered a PEP?

As described above, a PEP is someone who occupies a prominent public position. Once a person no longer holds that position, they are no longer considered a PEP. However, B2B shall continue to apply a risk-based approach to determine whether an existing customer who is no longer a PEP should continue to be treated as a high-risk customer.

Higher risk PEPs are also more likely to continue to pose a ML/TF risk after they cease holding a public position. As such, B2B may choose to undertake enhanced customer due diligence (ECDD) for a longer period for a former PEP.

A reporting entity should have a risk management system to determine if a person is a PEP. If the customer is a PEP, a reporting entity must adequately identify the person and verify his or her identity, take reasonable measures to establish the source of wealth and the source of property, and regularly monitor the account. Approval of senior management should be obtained before establishing a business relationship with the customer.

The following documents should be collected from any potential customer identified as a PEP:

- Proof of Identification: A valid ID or Passport
- Proof of Address not older than 3 months: Utility bill, bank statements, telephone bill, or any other reasonable proof of Address.
- A PEP Declaration Form.
- Proof of Source of funds
- CV
- Bankers Reference letter
- Legal or Tax Advise

4.7. Professional Intermediaries and Brokers

As part of the normal course of business, and upon authorization, the Company may outsource a number of functions to third parties and also enter into agreements with service providers. It is clarified that the agreements which the Company will conclude with the service providers as well as the names of the service providers will be submitted to the FSA.

The selection of third-party providers will be subject to the due diligence undertaken by the Company regarding the selection, appointment, and periodic reviews of the third parties with which the Company

will cooperate as well as based on the following criteria taken into account by the Company prior to the establishment of a business relationship with the third-party/provider:

- **Regulatory Status of the Provider (if applicable)**
- **Functionality**
- **Pricing/Commercial Terms**
- **Support**

Upon commencement of business relationship, the Company's personnel will be in communication with the relevant staff member(s) from the service provider(s) as part of their day-to day tasks and where required as per the examples below:

Banking/Payment Service Providers (PSPs)

The Company's Head of Accounting will act as the liaison as regards the Credit Institution(s) and PSP(s) (via the relevant Bank/PSP officer) with which the Company will maintain accounts with.

Liquidity and Platform Providers

The Company's Head of Dealing Room will be in communication with the relevant person from the Platform Provider for any matters related to the operation of the platform operated by the Company.

In addition, Head of Dealing will be interacting with personnel from the Company's Liquidity Provider(s) in relation to inter alia placing client orders and receiving order execution confirmations.

4.8. Ongoing transaction monitoring

B2B practices ongoing transaction monitoring for all its customers regardless of risk category. The transaction monitoring system is set to identify any transaction that appears to be suspicious, complex, unusual and have no apparent visible economic or lawful purpose. In addition to transaction monitoring, the Company has also implemented customer monitoring process where it monitors its relationship with its customer ensuring that the customer's activities being conducted are consistent with The Company's knowledge of the customer, the customer's business, source of funds and risk profile.

Customer service representatives will monitor the client's day-to-day activities and ongoing customer due diligence. Any and every transaction, payment, document that would not fall within the expected

associated with certain clients should be singled out and further examined by the AML/CFT Compliance Officers.

The initial or ongoing due diligence and monitoring may give rise to concerns requiring a review. The following are examples of circumstances which may give rise to such concerns:

a. Client's refusal to disclose details concerning business activities, e.g., unwillingness to disclose the source of funds or wealth or unwillingness to provide names of and other information on owners and other people with significant control over the business entity,
b. the behavior of the customer diverges from previous pattern or stated pattern, e.g., an inactive account suddenly becomes active with large transactions,
c. a prospective customer promises a trading volume, which does not make economic sense in the light of his background and other activities,
d. the purpose and intent behind the transaction or relationship is unclear, e.g., when the commercial rationale for certain service is missing or weak,
e. the representative suspects on reasonable grounds that the customer is not the person they claim to be or that the customers agent is not the person they claim to be,
f. there is suspicion on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence of financing of terrorism.

The assessment as to what constitutes suspicion shall be based on the information about the client received by the customer service representative handling the matter, and the scope of the client's business, along with the representatives general knowledge of deviating or suspicious transaction or activity patterns.

If the result of a review gives rise to an actual or potential suspicion related to Money Laundering, the representative shall immediately report the issue to compliance function, which shall initiate an investigation and decide whether to report the issue to the regulator through the raising of a suspicious transaction report.

B2Bs ongoing customer due diligence (OCDD) procedures should be able to detect whether any of its existing customers have a change in risk category; e.g. change in jurisdiction or become PEPs since they originally became a customer. If an existing customer does undergo a change in risk category, the reporting entity is required to update the customer's status, undertake enhanced customer due diligence and adjust its transaction monitoring processes. B2B may be alerted to a customer's change in status during the periodic review exercise undertaken by the compliance manager whereby updated customer information is requested.

5. SUSPICIOUS TRANSACTION REPORTS (STRS)

B2B's staff (including the AML/CFT compliance officer) who report a transaction or activity as suspicious are not necessarily expected to know or to establish the exact nature of any criminal offence the customer may be involved in. Further, B2B staff would not be expected to know or to establish that particular funds or property have been acquired through illicit or criminal means.

Once suspicious conduct is identified, employees must immediately bring it to the attention of the CO.

Client transactions or activity that have been identified as unusual or suspicious must be promptly reviewed and evaluated by Compliance to determine an appropriate course of action. This may include, but is not limited to, one or more of the following:

- Reporting the suspicion to the authorities;
- Terminating the business relationship;
- Requesting- further information or KYC documentation to try to alleviate concerns; or
- Doing nothing further.

5.1. Submission of information to the FIU

The Compliance Officer would carry out a review of the transaction and if he or she agrees that the transaction is likely to be involve in laundering or fraud, and if any adverse is found, the CO would submit a STR to the Seychelles Authorities (FIU) within two (2) business days through the FIU platform - GoAML Home (fiu.sc)

Prior to submitting a Suspicious & Unusual Transaction Report, a record of the submitted report must be captured in the Suspicious Transaction Report Register.

Below is a non-exhaustive list of information to be taken into consideration:

(a) the identity of the account holders

(b) the identity of the Beneficial Owners of the account

(c) the identity of the persons authorised to manage the account

(d) data of the volume of funds or level of transactions flowing through the account

(e) connected accounts

(f) in relation to specific transactions:

- the origin of the funds
- the type and amount of the currency involved in the transaction
- the form in which the funds were placed or withdrawn, for example cash,cheques, wire transfers
- the identity of the person that gave the order for the transaction
- the destination of the funds
- the form of instructions and authorization that have been given
- the type and identifying number of any account involved in the transaction

6. Tipping Off

Any staff (without prejudice to the generality of the foregoing a reporting entity, its officers, employees, or agents) who, knowing or suspecting that:

- a suspicious transaction report or a direction of the FIU has been or may be made or that further information has been given under s.48 of the AML Act,
- a reporting entity has formed a suspicion in relation to a transaction for the purpose of S. 48 of the AML/CFT Act 2020,
- any other information from which the person to whom the information is disclosed could reasonably be expected to infer that a suspicion has been formed or that a suspicious transaction report has been or may be made,
- a search warrant is to be issued or has been issued,
- an application is to be made, or has been made, under the AML Act for a production order,
- an investigation has commenced concerning the circumstances that gave rise to the suspicious transaction report, the warrant or the production order;
- makes any disclosure which could or may or be likely to prejudice the implementation of the warrant, the making available of the material in accordance with the production order, or the investigation,

commits an offence and is liable on conviction to imprisonment up to six months or to a fine not

exceeding SCR200,000 or to both.

7. Malice Reporting

Any staff of the company who willfully gives any information to the FIU or to an authorised officer, knowing such information to be false, commits an offence and is liable on conviction to a fine up to SCR200,000 or to imprisonment up to six months or to both.

Can a reporting entity continue a business relationship with a customer if the reporting entity has formed a suspicion about that customer?

The AML/CFT Act does not direct reporting entities to stop providing designated services to, or terminate a business relationship with, a customer, even if the reporting entity has formed a suspicion about that particular customer. B2B's senior management will assess and determine whether to terminate the relationship with the customer based on their risk-assessment, procedures and controls.

If B2B does decide to terminate the business relationship with the customer, the staff handling the customer relationship **must not disclose to the customer** that it has formed a suspicion and/or raised a STR due to the suspicion as 'tipping off' the customer, is an offence under the AML/CFT Act. 'Tipping off' is explained in more detail below.

In the event that B2B's senior management decide to continue business relationship with customer, B2B will continue to comply with the AML/CFT Act in all future dealings with that customer, which may include submitting additional STRs. Subsequent transactions or matters involving the customer must only be reported if they meet the STR reporting criteria.

8. Compliance function in AML and CFT

The Company has established compliance function within the Company that directly reports to the Board of Directors, with specifically dedicated staff as AML & CFT Compliance Officers.

A compliance Officer shall be appointed as per the requirements of S. 34 of the AML/CFT Act 2020

8.1. Responsibilities of AML and CFT Compliance

Officer(s)

The responsibilities of the AML & CFT Compliance Officer are:

a. monitoring compliance and adherence to the obligations of the AML and CFT Act;
b. receiving and investigating reports of suspicious matters activities;
c. adopting a risk-based approach to monitoring customer activity to identify suspicious activity;
d. ensuring that proper AML and CFT records are maintained;
e. reporting suspicious activity to the regulator;
f. providing advice internally to the different department that encounter AML/KYC issues;
g. receiving and carrying out directions or orders issued by Authorities;
h. liaison with regulatory bodies and law enforcement in respect of suspicious activity and threshold reporting;
i. preparation and review of AML Policy and Program;
j. overseeing communication and training for employees; and
k. submitting reports to the Board (at least annually).

The role of the Compliance Officer shall also cover all that is listed under S. 34(2) of the AML/CFT Act 2020.
The AML & CFT Compliance Officer is authorized and have full capacity to act independently in order to fulfil the commitments of his/her role as well as receive all information necessary to carry out the compliance functions.

The compliance function must be consulted prior to The Company:

a) introducing a new designated service to the market;
b) introducing new methods of delivery of a designated service; and/or
c) introducing any new or developing technology used for the provision of designated services to enable the AML and CFT Compliance Officer(s) to identify any significant changes in ML/TF risks and to formulate controls to mitigate and manage those risks.

8.2. KNOW YOUR EMPLOYEE

A Know Your Employee (“KYE”) program means that the Company has a program in place that allows it to understand an employee’s background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job descriptions, codes of conduct and ethics, levels of authority, compliance with personnel laws and regulations, accountability, monitoring, dual control, and other deterrents should be firmly in place.

Background screening of prospective and current employees, especially for criminal history, is essential to keeping out unwanted employees and identifying those to be removed.

8.3. ML and CFT Training Program

Appropriate training with regard to money laundering and terrorist financing is vital in managing the ML/TF risk. Accordingly, all employees of The Company are required to undergo training in AML and CFT laws and The Company's internal policies.

The training can be conducted by internal or external personnel (by contracted training organizations). At a minimum the AML and CFT training program will be designed to enable employees to understand the following:

a) the AML and CFT Policy;
b) the AML and CFT Program;
c) the obligations of The Company under the AML and CFT Act and underlying legal requirements;
d) the types of ML/TF risk The Company might face and the potential consequences of such risks;
e) how to identify signs of ML/TF that arise during the course of carrying out their duties;
f) escalation procedures i.e., what to do once a ML/TF risk is identified;
g) what employees' roles are in the firm's compliance efforts and how to perform them i.e., the processes and procedures relevant to each person's role;
h) the company's record keeping and record retention policy; and
i) the consequences (including civil and criminal penalties) for non- compliance with the AML and CFT Act and supporting Rules.

the following documents shall be referred to for most AML/CFT trainings :

- Provisions of the AML Act and its Guidelines
- The Company’s AML Policy & Manual and any updates that may follow
- The Company’s Internal Supervision, Control, and Compliance documented Procedures
- Updates and changes on the AML/CFT Act 2020 and its Guidelines

Updates and changes on Internal Supervision, Control, and Compliance documented Procedures
Records of training must be maintained to demonstrate that the person/s attended the training session/s, the dates of training, a brief description of the subject matter of the training provided and the number of hours (or level of accreditation) for attending the course/session/seminar.

Annually, all employees dealing with client-related matters or, who, due to the nature of their position, have special needs of AML knowledge, shall undergo training, be updated and/or informed regarding important and relevant AML regulations and relevant internal procedures as appropriate. All newly on

boarded Representatives shall undergo training within 3 (three) months.

8.4. Screening Procedures of Personnel Recruitment

Before extending an offer of employment, the Human Resources department, in collaboration with the Compliance Officer, shall conduct pre-employment screening on all potential candidates. This screening will include a thorough review of the candidate's qualifications, work history, references, and background checks. Ongoing screenings for existing employees are conducted periodically. Confidentiality and record-keeping protocols are emphasized, and non-compliance with AML/CFT regulations can result in disqualification or disciplinary actions. Reporting any suspicious findings to the Compliance Officer is mandatory, and regular reviews and training are integral to the procedure's effectiveness and alignment with regulatory requirements.

9. Confidentiality, Security and Protection.

The Company, its officers and all its employees shall at all times preserve the confidentiality of all Information communicated and documents provided by its clients or potential clients, as well as their privacy, except where the Company is required by the law to report to relevant authorities any suspected illegal activities by clients.

The Company shall ensure that its IT systems and internal procedures are secure against data leaks and shall take all measure to protect the confidentiality of its clients or potential clients.

Any actual or suspected breach of Confidentiality, Privacy, Security or Protection shall be communicated immediately to the Compliance Officer(s).

10. Period/Frequency of Review of the Manual

This AML/CFT Manual shall undergo regular reviews to ensure its continued relevance and effectiveness in combating Money Laundering (ML) and the Financing of Terrorism (TF). The frequency of these reviews will be as follows:

A comprehensive review of the AML/CFT Manual will be conducted annually. This annual review will encompass a thorough examination of all policies, procedures, and controls to assess their alignment with current regulatory requirements, industry best practices, and any emerging risks.

In addition to the annual review, the AML/CFT Manual may be subject to triggered reviews in response to significant changes in regulatory requirements, business operations, or the ML/TF

landscape. Triggered reviews will ensure immediate adjustments are made when necessary.

The AML/CFT Manual will be updated periodically to reflect any amendments to relevant laws, regulations, or guidelines. These updates will be conducted promptly to maintain compliance with the latest legal and regulatory developments.

The responsibility for overseeing these reviews and updates rests with the Compliance Officer, who will work in coordination with relevant stakeholders to ensure the AML/CFT Manual remains a dynamic and robust tool in our commitment to combating ML and TF. Any changes or updates resulting from these reviews will be communicated to all employees and relevant parties, and appropriate training and awareness programs will be conducted to ensure continued adherence to the revised policies and procedures.

Following each review and update of this AML/CFT Manual, a copy of the updated manual shall be promptly submitted to the Financial Services Authority of Seychelles (FSA).

Appendix A

Employee Acknowledgement of AML Manual

Employee Information:

Name: _____
Email ID: _____
Department: _____
Date of Acknowledgement: _____

I, the undersigned, hereby acknowledge that I have received and read the Anti-Money Laundering (AML) Manual of Phoenix Limited and understand its contents. I also confirm my commitment to comply with the policies and procedures outlined in the AML Manual.

Key Acknowledgements:

1. I have received a copy of the AML Manual.

2. I have read and understood the AML Manual.

3. I am aware that compliance with the AML policies and procedures is mandatory.

4. I understand that any questions or concerns regarding the AML Manual can be addressed to the Compliance Officer

I further acknowledge that failure to comply with the AML policies and procedures may result in disciplinary action.

Employee Signature: _____ Date: _____