Trillium Financial Broker

AML Policy

TRILLIUM FINANCIAL BROKER

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

Regulated by the Financial Services Commission of Mauritius

Table of Contents

1 INTRODUCTION

1.1 DEFINITIONS AND ABBREVIATIONS

The abbreviations and words listed below come with their respective definitions and interpretations in the text:
“The Company”- Trillium Financial Broker
“AML/CTF” – Anti-Money Laundering and Counter-Terrorism Financing
“DD” – Due Diligence
“EDD” – Enhanced Due Diligence
“MLRO” - Money Laundering Reporting Officer
“Money Laundering” – procedures intended to conceal the true origin of criminal proceeds, making these appear to originate from a legitimate source
“CO” – Compliance Officer
“KYC” - Know Your Client
“PEP” – Politically Exposed Person

1.2 KEY AML CONCEPTS

Money laundering entails concealing the origin, ownership, or intended purpose of funds derived from illicit activities, such as corruption, fraud, and tax evasion. Trillium Financial Broker is committed to aiding government endeavors in combating money laundering.
Five specific offenses outlined in the Regulations apply universally to employees of any financial services company or those handling money in any capacity:

- Acquisition, use or possession of criminal property
- Engaging in the acquisition, use, or possession of criminal assets is considered a criminal offense.
- Handling the proceeds of corruption
- Corruption committed by public sector employees, officials, and politicians is a grave crime; likewise, dealing with the illicit gains resulting from such corruption is also considered a criminal offense.
- Arrangements relating to criminal property

In the context of this Company, engaging in any arrangement connected to criminal property, which encompasses granting permission or providing assistance in its acquisition, retention, or utilization, constitutes a serious criminal offense. However, the Company affords its employees the opportunity to defend themselves if they can demonstrate that they acted responsibly by promptly reporting their knowledge or suspicion to the Anti-Money Laundering Compliance Officer (AMLCO) or the relevant authority in accordance with the prescribed procedures.

Tipping – off
Disclosing any information that could reasonably be deemed to influence an investigation into money laundering is deemed a criminal offense. Such a tipping-off offense occurs when an individual is aware of or suspects that an internal or external disclosure has taken place and, despite this knowledge, divulges information to another person or reveals the existence of an ongoing or contemplated investigation.

Failure to Report

Any individual who becomes aware of or suspects money laundering, or possesses information that could reasonably lead to such knowledge or suspicion, is legally obligated to report it to the competent authority or authorities.
It is crucial to emphasize that reporting knowledge or suspicion of money laundering should never be perceived as a breach of financial companies' requirements to uphold client confidentiality. Even in cases where the reported knowledge or suspicion is not substantiated during investigation, the disclosure is limited to only the reporter and the Anti-Money Laundering Compliance Officer (AMLCO), thus preserving the confidentiality of any individual who might be incorrectly accused.

1.3 REGULATION OVERVIEW

The Company is dedicated to maintaining the utmost standards of Anti-Money Laundering (AML) compliance and Counter-Terrorism Financing (CTF). This comprehensive AML/CTF Policy has been meticulously crafted to establish a robust framework for the Company's operations, ensuring a steadfast commitment to adhering to all applicable laws and regulations in force within Mauritius.
The prevention of money laundering and terrorism financing in Mauritius is governed by a set of definitive laws and regulations, which the Company is unwaveringly committed to observing and complying with at all times:

- Financial services Act 2007;
- Financial Intelligence and Anti-Money Laundering Act 2002;
- Code on The Prevention of Money Laundering & Terrorist Financing 2012;
- Other relevant acts, guidelines and regulations under the laws of Mauritius.

2 MONEY LAUNDERING PROVISIONS

2.1 SUSPICIOUS TRANSACTIONS REPORT (‘STR’)

General
As per FATF Recommendation 20, if a financial institution holds suspicions or has reasonable grounds to believe that funds are derived from criminal activities or connected to terrorist financing, it is legally obligated to promptly report these suspicions to the financial intelligence unit.
A STR is often identified by its inconsistency with a customer's known legitimate business or their typical transaction history, as observed through customer activity monitoring. Consequently, particular emphasis will be placed on assessing factors related to the customer's business and their unique requirements. To ensure the efficacy of our anti-money laundering efforts, every member of the staff is entrusted with the responsibility of promptly reporting any knowledge or suspicion of money laundering. Additionally, continuous monitoring of transactions is a fundamental aspect of our commitment to combat financial crimes and maintain the highest standards of compliance.
Internal suspicious and related transaction reports must be promptly and exclusively disclosed to the Money Laundering Reporting Officer (MLRO). The MLRO will attend to the report immediately and initiate a thorough investigation to determine if the internal transaction is in violation of any pertinent laws and regulations.

Reporting Mechanism
Any employee who suspects money laundering is obligated to report it. However, it goes further than this; if reasonable grounds indicate a suspicion of money laundering, failing to acknowledge and report it would constitute an offense. Therefore, having clear and robust KYC policies is vital in

preventing money laundering and related activities. It is imperative that all employees share the Company's unwavering commitment to these policies, ensuring a unified and effective approach in combating financial crimes and maintaining regulatory compliance.
Employees, including those in the Backoffice, must report any suspicious transactions to the MLRO within two days to avoid delays. The STR must be documented appropriately before the MLRO forwards it to the Regulatory Bodies. The Company ensures that the reporting mechanism for STR operates in a secure environment to maintain confidentiality and preserve secrecy.
The following list of common questions can aid in identifying potentially suspicious transactions:

a. Does the transaction align with the client's usual activities?
b. Is the transaction size significantly different from the client's typical profile?
c. Does the transaction deviate from the client's historical transaction patterns?
d. Are there any links to other suspicious transactions?
e. Does the client's suggested payment method appear unusual?
f. Does the transaction, along with others, indicate a notable change in the client's usual transaction pattern?

The Company is required to retain records of suspicious transaction reports for a minimum of 7 (seven) years. The Company must send a report to the Financial Intelligence Unit Republic of Mauritius at the provided address and fax number.
To: Financial Intelligence Unit
7th Floor Ebene, Heights
34, Ebene Cybercity Ebene
Mauritius
Or send complete form by Fax (230) 466 2431

Customers will not be informed about their transactions being potentially suspicious or under investigation by the Company.
Reporting information that gives rise to suspicion or reasonable grounds for suspicion of money laundering is a statutory and regulatory obligation for all staff of the Company. Even if a staff member does not personally know or suspect, but reasonably should have known or suspected money laundering or a related breach, failing to report it is considered an offense.
Transaction-based monitoring will be carried out within the relevant business units of the Company. Account activity will be closely monitored to identify and comprehend the typical pattern of transactions, including size, volume, type, and geographical locations. Each transaction will be assessed for consistency with the usual activity pattern, and any transaction that appears financially illogical or raises suspicion for a particular customer will be flagged as potentially suspicious.
Special attention will be focused on any transaction exceeding USD 10,000 (or its equivalent in any other currency).
Industry-proven signs of suspicious activity that may indicate money laundering include the following examples:

- Same-day deposits and withdrawals.
- Transactions that deviate from usual patterns, lack financial sense, or lack a clear legal purpose.
- Conducting transactions without completing corresponding trading operations on the account.
- Unjustifiably heightened concern from a customer regarding the confidentiality of their identity, business type, or the source of their funds.
- A customer providing different and inconsistent information to different employees.

- A customer displaying a lack of knowledge about the industry they are involved in.

It is essential to note that the list of examples mentioned above is not exhaustive.
If an employee detects any suspicion of money laundering or has reasonable grounds to suspect a transaction's suspicious nature, they must promptly report it to the AML Compliance Officer. The AML Compliance Officer may then instruct the employee to aid in further investigating the client's activity, which may involve gathering additional information from the customer or relevant third parties. Consequently, the trading account may be classified as a high-risk account. As a result, all funds transfers or requests for transfers from this account will be subject to heightened scrutiny by the AML Compliance Officer before being processed.

2.2 IDENTIFICATION PROCEDURES

The Company is obligated to ensure, as promptly as reasonably possible after the initial contact with a customer or counterparty (referred to as an "applicant"), and before remitting any money to a third party, that satisfactory evidence of the applicant's identity is obtained. The Company may also take other measures that will yield satisfactory evidence of the applicant's identity. Furthermore, if a client appears to be acting on behalf of another individual, the identification requirements extend to obtaining sufficient evidence of that third party's identity as well.
If the Company does not receive satisfactory evidence of a customer's identity, it will refrain from proceeding with any further business and terminate any existing understanding with the client. This will be done unless the Company has duly informed the Mauritius FSC. In the event of knowledge or suspicion of money laundering, the Company will promptly report it in accordance with the established procedures to the MLRO.

2.3 METHODS OF IDENTIFICATION

The Company will take necessary measures to verify the identity of a real person or legal entity and ensure that the applicant is indeed that individual or organization. If the Company relies on any third party to identify or confirm the applicant's identity, the ultimate legal responsibility to ensure the adequacy of the procedures and evidence obtained remains with the Company.
Since no single form of identification can be entirely foolproof in verifying a person's genuine identity, the identification process must be cumulative. The Company will not solely rely on a single document or data source (except for a database constructed from multiple reliable sources) to verify both the name and permanent address of an applicant.
The Company will diligently implement all necessary measures, in accordance with applicable laws and regulations issued by regulatory authorities, to verify the identity of its clients. Additionally, when applicable, the Company will also make efforts to ascertain the identity of the respective beneficial owners.

2.4 CLIENTS DUE DILIGENCE (‘CDD’)

As per FATF Recommendation 10, financial institutions are required to prohibit the maintenance of anonymous accounts or accounts with obviously fictitious names. In addition, these institutions must conduct customer due diligence (CDD) measures when establishing business relations, carrying out occasional transactions, when there is suspicion of money laundering or terrorist financing, and when there are doubts about the accuracy or sufficiency of previously obtained customer identification data.
Before executing any transaction for a new client, the Company must ensure the following procedures are in place and carried out:

a. AML procedures, including client identification, record-keeping, detection and monitoring of unusual or suspicious transactions, and internal reporting and control, as required.
b. Employees are aware of their responsibilities and fully understand the Company's procedures.
c. Relevant training is undertaken to equip employees with the necessary knowledge and skills to comply with AML regulations effectively.
d. All pertinent requests from external sources are directly forwarded to the MLRO for appropriate action.

Upon receiving supporting documents related to a new client's identity, the Company must thoroughly verify that they unequivocally establish the existence of the client as a genuine natural or legal entity, confirming their claimed identity. While the Company may occasionally use third-party sources as part of its fact-checking process during client onboarding, it bears the ultimate legal responsibility to ensure that the checks conducted are satisfactory and accurate.
In cases where the submitted identification is found to be incomplete, inaccurate, or otherwise insufficient, the Company will not proceed with opening an account for the client. In more serious instances where there are suspicions of money laundering, identity fraud, or other crimes, rather than simple carelessness or misunderstanding, the MLRO will promptly inform the relevant authority.
Due to the fact that no single identification can provide absolute certainty, the Company adopts a robust approach by using multiple documents to verify every new client's full name and address. As part of the Company's due diligence policy, five key pieces of information are collected and actions conducted:

a. Establish the source of the applicant's funds.
b. Determine the applicant's net worth.
c. Identify the specific source of the funds to be deposited.
d. Obtain source references or other relevant documents that verify the applicant's good reputation, where applicable.
e. Conduct comprehensive background checks to further validate the applicant's credentials.

Indeed, the identification process for individual clients and corporate clients differs slightly due to the complexities involved in establishing the identities and reputations of companies.

2.5 IDENTIFICATION OF CLIENT

2.5.1 Individual customers

The Company will verify the identity of individual customers to its satisfaction by referring to official identity papers or any other suitable evidence depending on the circumstances. The information required for identity verification will encompass, but not be limited to, the customer's full name, date of birth, nationality, and complete residential address.
Identification documents provided by clients must be current and valid at the time of the account opening.
To verify personal information, the following documents are required:

- A valid passport.
- A national identity card or its equivalent in the relevant jurisdiction.
- A document that confirms the residential address, such as a utility bill, bank statement, or an acknowledgement of address issued by a relevant official.

2.5.2 Corporate customers

In cases where the applicant company is listed on a recognized or approved stock exchange, or there is independent evidence confirming it as a wholly owned subsidiary or under the control of such a listed company, no further steps to verify identity over and above the usual commercial checks and due diligence will normally be required.
When dealing with an unquoted company, the Company will implement a specific procedure to identify and verify its existence, good standing, and the authority of individuals acting on its behalf. The required documentation for this purpose may vary depending on the specific jurisdiction but typically includes:

- Certificate of incorporation or certificate of trade, or the equivalent, to evidence that the company is legally incorporated in a particular jurisdiction under the relevant legislation.
- Certificate of Incumbency or a similar document that lists the current directors of the company.
- Statutes, Memorandum and Articles of Association, or equivalent documents that confirm the authority of the company's officers to legally bind the company and specify the manner in which this can be done.

Additionally, an extract from the Commercial Register of the country of incorporation may also be utilized to confirm the aforementioned information if such details are included in the extract.

2.5.3 Beneficial owners

KYC and due diligence procedures for account owners vary between individual clients and institutional clients. When dealing with individual clients, the Company must ensure that the client applying is acting on their own behalf and not on behalf of another natural or legal person.
For institutional clients, the Company must obtain a comprehensive understanding of the applicant company's structure based on the documents provided. This includes knowing the source of funds for the account, identifying the main owners or singular owner of the company's stock (if applicable), and verifying the identities of the company's board of directors or equivalent individuals who have ultimate control over the applicant company's finances. The AMLCO plays a crucial role in making informed judgments on whether additional information is necessary to ensure regulatory compliance and mitigate potential money laundering risks.
For the purpose of due diligence, the Company will accept documents certified by the following certifiers:

- A notary public or any other authority with equivalent power to certify copies of documents in the relevant jurisdiction.
- A relevant state official, which may include a judge, police officer, consular official, and others with the authority to certify documents.
- An authorized financial institution.

If any document related to the corporate entity, such as an extract from the Commerce Register, is accessible online through an official website of the relevant state authority, the Company may refer to the online version of the document. However, to ensure compliance with record-keeping requirements, a printout of the online document must be made by a staff member of the Company and stored in the respective client file.
Clients may be asked to provide relevant contact details, including their phone number and email address.

The Company may request the following source documents for the identification of ultimate beneficial owners and controllers, but this list is not exhaustive. Depending on the circumstances, the Company may utilize other appropriate means to verify the client's identity upon registration.

Type of legal person/legal arrangement	Information relating to beneficial ownership	Source documents
Private and public companies/Bodies corporate/ Partnership	(i) Legal vehicle (e.g. corporate, partnership etc)	• Certificate of incorporation • Certificate of registration • Company constitution • Partnership Agreement • Minutes of Board meeting
Government-linked companies	(i) Shareholding including information on parent company and subsidiaries information (ii) Direct or indirect ownership (iii) Relationship to conglomerates/ corporate groups (iv) Company tree	• Directors and shareholder's resolution • Partnership agreement • Appointment/Authorisation letter • Senior management list • Company's annual report and annual return • Joint venture agreement, shareholder's agreements and other related agreements • Director nomination agreement • Register of member including BO • Any other source documents that sufficiently identifies the beneficial owner
Trust arrangement	(i) Parties to the trust (ii) Persons involved in the trust establishment (iii) Administrator of the trust (iv) Type of trust	• Trust deed • Trust registration document
Cooperatives	(i) Management of the cooperatives (ii) Rules governing the cooperatives	• Registration form of the Cooperatives • By-laws of the cooperative • Minutes of General Meeting
Clubs/Societies/ Foundations/ Charities/ NGOs	Rules governing the clubs/societies/ foundations/	• Constitution/ charter/ rules • Registration form • Minutes of meeting

	charities/NGOs	● List of members of committee

The identification of beneficial owners of a legal person or legal arrangement depends on the type and may be determined based on the following relationships:

Type of legal person/legal arrangement	Relationships to be determined, if any
Companies (Private & Public)	● Shareholders ● Senior management ● Joint venture agreement ● Persons with voting rights ● Nominee directors/ shadow directors ● Persons with power to appoint or remove directors ● Other persons with interest within the company
Partnership	● Partners within the partnership ● natural persons with effective control er the partnership
Government Linked companies – Government investment linked companies, state-based company etc.	● Person authorised in the government to exercise or influence decision making on the GLC ● Other persons who exercise or influence decisions over the GLC
Clubs/ Societies/ Foundations/ Charities/ NGOs/ Cooperatives	● Office bearer (e.g. president, secretary, treasurer or other committee) ● Senior management/ management team ● Other member with effective control over the club/ societies/ charities/ foundations/ cooperatives
Trust arrangement	● Settlor ● Trustee ● Protector ● Beneficiaries or class of beneficiaries ● Other natural persons with effective control over the trust

2.6 MONITORING AND UPDATE

Effective ongoing monitoring and documentation of customer accounts and transactions are crucial for maintaining robust KYC protocols. By understanding customers' normal transaction

patterns, the Company can identify and report any suspicious activities, ensuring compliance with regulatory obligations and mitigating risks associated with money laundering, fraud, and illicit activities. Adjusting the monitoring process based on account risk levels enhances the overall effectiveness of anti-money laundering and risk management efforts, fostering a secure and compliant business environment that builds customer trust and upholds the integrity of the financial system.
The Company has implemented comprehensive systems to identify any unusual or suspicious patterns of activity, utilizing specific account category limits as reference points. Transactions exceeding these limits are closely monitored, especially those showing signs of lacking economic or commercial logic or involving substantial cash deposits, as they may indicate potential suspicious activity. Higher risk accounts are subjected to key indicators, considering factors such as the customer's country of origin, source of funds, transaction types, and other relevant risk factors.

2.7 SECURITY MEASURES

2.7.1 High – risk countries

The Company will implement enhanced due diligence measures for clients and beneficial owners residing in countries identified by credible sources as having weak anti-money laundering standards or representing a high-risk for criminal activities. Additionally, increased scrutiny will be applied to transactions conducted by clients or beneficial owners from these countries.

2.7.2 Offshore jurisdictions

The due diligence procedures outlined in these guidelines cover risks associated with entities organized in offshore jurisdictions. Nonetheless, the Company will impose even stricter standards for transactions conducted by clients or beneficial owners headquartered in such jurisdictions.

2.7.3 High - risk countries, client and activities

Applicants from countries identified in the FATF blacklist, which have insufficient AML standards, will be subjected to minimum higher scrutiny by the Company. However, applications from residents of countries classified under the category 'call to apply counter-measures' will not be accepted.
The measures outlined in this document adequately address the risks associated with applicants from offshore jurisdictions. However, if such clients are accepted, their transactions will be subject to heightened scrutiny by the Company. This also applies to clients whose wealth is known to be derived from activities susceptible to money laundering.
The Company will stay vigilant for any changes announced by the FATF regarding the list of high-risk countries. In the event of any updates, the Company will promptly carry out enhanced due diligence for clients originating from the countries listed.

2.7.4 Politically Exposed Persons (PEP)

Under FATF Recommendation 12, financial institutions are mandated to take additional measures concerning foreign politically exposed persons (PEPs) who are either customers or beneficial owners. In addition to normal customer due diligence, financial institutions must:

a. Implement appropriate risk-management systems to identify whether the customer or beneficial owner is a PEP.

b. Obtain senior management approval before establishing new business relationships with PEPs or continuing existing ones for current customers who subsequently become PEPs.
c. Undertake reasonable steps to ascertain the source of wealth and funds of the PEP.
d. Conduct enhanced ongoing monitoring of the business relationship with the PEP.

Financial institutions are obligated to implement reasonable measures to ascertain whether a customer or beneficial owner is a domestic politically exposed person (PEP) or an individual who holds or has held a prominent function within an international organization.
The Company will adopt the following approach concerning the accounts of "Politically Exposed Persons" (PEPs):
Establishing a Business Relationship or executing occasional transactions with individuals holding significant public positions and their closely related natural persons can subject the Company to heightened risks, especially if the potential client seeking to establish such a relationship or conduct transactions is a PEP, a member of their immediate family, or a close associate known to be associated with a PEP.
The Company's general policy is to refrain from conducting business with Politically Exposed Persons (PEPs). However, if an existing client becomes a PEP during the ongoing monitoring process, the MLRO will promptly report the case to the Board for their decision. The Board will assess the situation and determine whether to proceed with the client or terminate the relationship, based on a comprehensive risk evaluation. If the Directors decide to continue the business relationship, the MLRO will exercise Enhanced Due Diligence measures for the respective client.

2.7.5 On-Going Monitoring

The constant monitoring of clients' accounts and transactions is a crucial element in effectively controlling the risk of Money Laundering and Terrorist Financing.
In this regard, the MLRO holds the responsibility for both maintaining and further developing the ongoing monitoring process of the company. As part of the internal control framework, the Internal Auditor, once appointed, shall conduct an annual review of the company's procedures pertaining to the ongoing monitoring process.
The procedures and intensity of monitoring clients' accounts and examining transactions will be tailored according to the level of risk associated with each client. The monitoring process shall include the following steps:

I. Identification of:
- Transactions that, due to their nature, may be associated with money laundering or terrorist financing.
- Unusual or suspicious transactions that deviate from the economic profile of the client, warranting further investigation.
- In the event of any unusual or suspicious transactions, the relevant employee shall promptly communicate with the MLRO.

II. Investigation of unusual or suspicious transactions by the MLRO. The outcomes of these investigations will be documented in a separate memorandum and retained in the files of the respective clients.
III. Verification of the source and origin of funds credited to accounts, ensuring transparency and compliance with anti-money laundering standards.
IV. Utilization of appropriate IT systems to facilitate efficient monitoring and analysis of client activities, enabling the timely detection of potential risks and red flags.

2.8 EMPLOYEE TRAINING AND AWARENESS PROGRAMMES

The Company will conduct regular awareness and training programs on AML/CFT, ensuring that employees stay informed about the latest developments and best practices in the field. These training programs may be supplemented with virtual refresher courses at appropriate intervals to reinforce the knowledge and skills necessary to identify and address potential money laundering and terrorist financing risks effectively.
The Company shall communicate to all employees that failure to observe the AML/CFT requirements can result in personal liability.
The Company is committed to ensuring that its AML/CFT policies and procedures are readily accessible to all employees. To achieve this, the Company will make available the following documented AML/CFT measures:

a. The relevant documents on AML/CFT issued by Mauritius FSC, ensuring that employees have access to up-to-date regulatory guidelines and requirements.
b. The Company's internal AML/CFT policies and procedures, providing comprehensive guidance on the identification, prevention, and reporting of money laundering and terrorist financing activities within the Company's operations.

The training will cover the detection of money laundering and terrorist financing activities, as well as the specific risks of ML/TF identified by the Company.

2.9 MANDATORY REPORTING OBLIGATION

All staff members are bound by legal and regulatory obligations to promptly report any information they become aware of that might indicate potential money laundering. This duty applies even if they do not hold strong suspicions but have reasonable cause to believe there could be an issue. The Company recognizes the significance of continuous transaction monitoring to detect any signs of suspicious activity effectively. To combat money laundering successfully, the Company places utmost importance on understanding its customers, verifying their identities, and ensuring they engage in legitimate business practices while upholding the highest standards of integrity, consistent with the Company's values and principles.
Being aware of money laundering entails avoiding deliberate ignorance and refraining from neglecting reasonable inquiries, even when one is aware of circumstances that would raise suspicion in an honest person. It also means possessing knowledge of circumstances that would prompt an honest person to make necessary inquiries.
Having reasonable grounds to suspect money laundering involves applying an objective standard, devoid of personal beliefs or biases. It includes acknowledging and addressing red flags, conducting thorough investigations, and critically evaluating all available information and facts.
The Company is firmly committed to ensuring that its employees take all essential measures, tailored to the specific circumstances, to thoroughly understand the customer and the underlying purpose behind each transaction or request.

2.10 CONFIDENTIALITY

Reporting suspicions of money laundering serves as a defence against charges of Breach of Confidence. However, all media statements or public disclosures must be handled through the Money Laundering Reporting Officer (MLRO) or their deputy. All requests for information or statements should also be directed to the MLRO or their deputy for a response. Maintaining confidentiality during the investigation process is paramount, and employees must remember the

consequences of "tipping-off," which involves disclosing information that could affect an ongoing money laundering investigation.

2.11 INTERNAL REPORTING

All employees are required to promptly inform the MLRO of any suspicions of money laundering they may encounter. Refer to Appendix II.
When reporting a suspicion of money laundering, employees must carefully document all relevant details, including their name, client information, account details, and the reasons that raised the suspicion. Any internal inquiries related to the report, along with the reasoning behind submitting or not submitting the report, must be diligently documented.
The MLRO should always remind the reporting employee to exercise caution and avoid "tipping off" by refraining from sharing information about the report with any third parties. Confidentiality is paramount to ensure the integrity of the investigation and protect against potential interference.
The reporting requirement remains applicable even if a business or transaction is not completed due to circumstances that raise suspicion of money laundering.

2.12 HIGH RISK COUNTRIES

As per the guidance from FATF, financial institutions are obligated to implement enhanced due diligence measures for business relationships and transactions involving natural and legal persons, as well as financial institutions, from countries identified by FATF as requiring such measures. The application of these enhanced due diligence measures should be both effective and proportionate to the specific risks associated with each transaction or relationship.
If a client is identified as a citizen or resident of a country listed as high risk by FATF, the Company will conduct Enhanced CDD. As part of risk mitigation measures, the Company may take the following countermeasures for clients located in high-risk countries:

a. Limiting business relationships or financial transactions with the identified country or individuals located in that country.
b. Reviewing and amending, or if necessary, terminating correspondent banking relationships with financial institutions in the high-risk country.

The Latest list of high risk under FATF which dated 23 June 2023 are the following:

- Albania | Barbados | Burkina Faso | Cameroon | Cayman Islands | Croatia | Democratic Republic of the Congo | Gibraltar | Haiti | Jamaica | Jordan | Mali |
- | Mozambique | Nigeria
- | Panama | Philippines | Senegal | South Africa | South Sudan |Syria | Tanzania | Türkiye | Uganda | United Arab Emirates | Vietnam | Yemen
  and EU regulation (Delegated Regulation (EU) 2023/2070 - https://eur lex.europa.eu/eli/reg_del/2023/2070/oj):
  1. Afghanistan
  2. Barbados
  3. Burkina Faso
  4. Cameroon
  5. Cayman Islands
  6. Democratic Republic of the Congo
  7. Gibraltar
  8. Haiti
  9. Jamaica
  10. Jordan

11. Mali
12. Mozambique
13. Myanmar
14. Nigeria
15. Panama
16. Philippines
17. Senegal
18. South Africa
19. South Sudan
20. Syria
21. Tanzania
22. Trinidad and Tobago
23. Uganda
24. United Arab Emirates
25. Vanuatu
26. Vietnam
27. Yemen

2.13 RECORD KEEPING

Financial institutions and other financial sector businesses must uphold accurate and comprehensive record-keeping practices to adhere to relevant anti-money laundering (AML) laws and regulations. Maintaining proper records is vital in the efforts to identify and prevent money laundering and terrorist financing activities, and it also supports the facilitation of investigations conducted by law enforcement agencies.
The key elements of our record-keeping policy are as follows:

1. Customer Identification: We will keep records of customer identification information, such as names, addresses, and identification documents, in compliance with AML laws and regulations.
2. Transaction Records: We will maintain records of all customer transactions, including transaction details, parties involved, and the types of funds or assets used.
3. Risk Assessments: Records of risk assessments for customers and transactions will be kept, documenting the factors considered and conclusions reached.
4. Due Diligence: We will maintain records of due diligence measures, including enhanced due diligence (EDD), for higher-risk customers and transactions.
5. Suspicious Transaction Reports (STR): Records of any submitted STRs to regulatory authorities, including reasons for suspicion and investigation outcomes, will be retained.
6. Employee Training: Records of employee AML training, covering AML laws, our policies, and procedures, will be maintained.

All records will be stored securely and treated with utmost confidentiality. They will be retained for the duration specified by relevant AML laws and regulations. We will conduct periodic reviews of our record-keeping policies and procedures to ensure their ongoing relevance and effectiveness in combatting money laundering and terrorist financing.
Under the FATF guidelines, financial institutions are required to keep all relevant records related to transactions, whether they are domestic or international, for a minimum of five (5) years. These records must be comprehensive enough to facilitate prompt compliance with information requests from competent authorities. They should also allow for the reconstruction of individual

transactions, including details like amounts and types of currency used, if applicable. Maintaining such records is crucial as they may serve as vital evidence in prosecuting criminal activities related to money laundering and other financial crimes.

2.14 MANAGEMENT INFORMATION SYSTEM

The Management Information System available on our back-office system will provide us with a comprehensive view of our clients' transactions and details. It enables us to review client activities, detect any unusual transactions promptly, and monitor activities accurately, ensuring the system remains up-to-date and reliable. This system will be highly beneficial during stakeholder or regulatory inspections, as it allows us to provide a summary of client transactions when requested, making the process more efficient and transparent.

2.15 TARGETED FINANCIAL SANCTIONS ON TERRORISM FINANCING, PROLIFERATION FINANCING AND UNDER OTHER UN-SANCTIONS REGIMES

According to FATF recommendations, the targeted financial sanctions regime must adhere to the United Nations Security Council resolutions concerning the prevention and suppression of terrorism, terrorist financing, as well as the prevention, suppression, and disruption of the proliferation of weapons of mass destruction and its financing.

2.15.1 Maintenance of sanctions list

The sanctions database maintained by the Company will include, at a minimum, the following lists:

a. United Nations Security Council Resolutions (UNSCR) list.
b. Domestic List (specific to Mauritius).

The Company will conduct checks on each client against the UN list, which can be accessed on the official UN website (https://www.un.org). The UNSCR List will be regularly updated in the sanctions database and will remain there until the entities or designated persons or countries are officially delisted by the UNSC or its relevant Sanctions Committee and the delisting information is published on the UN website.
In addition to the UN list, the Company will also check for any relevant names on the Domestic List, which is provided by the Mauritius government. Regular checks will be conducted to ensure compliance with domestic regulations and to identify any potential sanctions-related issues.

2.15.2 Sanction screening - customer

The Company will conduct sanction screening as part of its CDD process and Ongoing Due Diligence for existing, potential, or new customers. This screening will involve checking each customer against both the UNSCR list and the Domestic list specific to Mauritius.
As a standard practice, the Company does not offer its services to individuals residing in countries identified by the FATF as high risk (latest 23 June 2023). However, in the event the Company decides to engage with clients from such high-risk countries, enhanced Customer Due Diligence (CDD) measures will be applied to both potential and existing clients. Moreover, the Company will refrain from providing services to countries that are locally regulated, subject to international sanctions, or considered non-cooperative jurisdictions with strategic Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) deficiencies.
The Company does not provide services to the persons residing in:

- Afghanistan

- Bosnia and Herzegovina
- Burundi
- Central African Republic
- Congo, Democratic Republic of the
- Guinea
- Guinea-Bissau
- Haiti
- Iran, Islamic Republic of
- Iraq
- North Korea
- Lebanon
- Libya
- Mali
- Myanmar
- Nicaragua
- Serbia
- Somalia
- South Sudan
- Sudan
- Syrian Arab Republic (Syria)
- Tunisia
- Yemen
- Zimbabwe
- Russian Federation
- Crimea
- USA

The list mentioned above is subject to updates at any time as determined by the Compliance Officer, with or without revising this document.

The Company does not facilitate transfers to or from accounts held in banks or payment institutions incorporated in the USA, its territories, or possessions, as well as countries identified

by the FATF as high risk and non-cooperative jurisdictions. Should the Company become aware, suspect, or have reasonable grounds to believe that a user is a resident of countries not served by the Company, all outstanding positions will be promptly closed, and the relevant account will be suspended.