COMPANY SERVICE PROVIDERS

This information sheet is meant to provide an overview of the Anti-Money Laundering/Counter Terrorism Financing (AML/CFT) obligations for Company Service Providers (CSP). These obligations are part of Mauritius' national framework aimed at combatting money laundering, associated criminal activity and terrorism financing.

The following summary of the legislative requirements under the Financial Intelligence Anti-Money Laundering Law 2002 (FIAMLA) applies to CSPs who prepare, or carry out, transactions for a client concerning the following activities:

- acting as a formation agent of a legal person;
- acting, or causing for another person to act, as a director, as a secretary, as a partner or in any other similar position of a legal person;
- providing a registered office, a business address or an accommodation, a correspondence or an administrative address for a legal person; or
- acting, or causing for another person to act, as a nominee shareholder for another person.

INTERNAL CONTROLS

You shall develop and implement policies, controls and procedures that will enable you to effectively manage and mitigate identified risks on the basis of the results of your money laundering/terrorism financing risk assessment.

The following elements shall be included in your internal controls:

- The appointment of a Money Laundering Reporting Officer (MLRO) and compliance officer at the appropriate level
- Programs for assessing risk related to money laundering (see section below)
- The development and application of written compliance policies, controls and procedures that manage and mitigate identified risks
- Implementation and documentation of an ongoing compliance training program
- A documented audit of the effectiveness of policies, controls and procedures, training program and risk assessment
- Ensure that your foreign branches and subsidiaries observe AML/CTF measures consistent with FIAMLA.

RISK ASSESSMENT

You shall undertake and document a money laundering and terrorism financing risk assessment, commensurate with the nature and size of your institution, to enable you to identify, assess, monitor, manage and mitigate the risks associated with money laundering and terrorism financing. The risk assessment should be conducted at least every two years.

REPORTING

Suspicious Transactions

You shall report to the Financial Intelligence Unit instances where you have reason to believe that a transaction may be related to money laundering, a criminal activity or terrorism financing, in the prescribed form immediately and, in any event, within 15 days from the day on which you become aware of the transaction.

Reporting under the United Nations (UN) Sanctions Act

You shall disclose any information to the National Sanctions Secretariat and the FIU related to a designated party or listed party under UN Sanctions Act 2019. Additionally, you shall not deal with or make available funds or other assets available to any designated or listed party under this Act.

Registration with Financial Intelligence Unit (FIU)

You shall immediately register with the FIU as soon as your operations begin or within such timeframes determined by the FIU. Information on how to register is available on the website of the FIU (www.fiumauritius.org).
In addition, a special helpdesk, for any assistance that you may require, has been set up. The contact details are as follows:

- email: goamlhelpdesk@fiumauritius.org
- Telephone: +230 454 1423

.

ON-GOING MONITORING

You shall establish monitoring programs in relation to complex, unusual or large or suspicious activities. The results of the monitoring should be documented.

ASCERTAINING IDENTITY AND CUSTOMER DUE DILIGENCE

You shall take reasonable measures to satisfy yourself as to the true identity of any client when:

a) establishing a business relationship with a customer;
b) carrying out a transaction in an amount equal to or above 500,000 rupees whether conducted as a single transaction or several transactions that appear to be linked;
c) doubts exist the veracity or adequacy of previously obtained customer identification information;
d) there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account.

Customer due diligence measures should include:

a) The identification of the customer and verification of that customer using reliable, independent source documents data or information
b) Identifying the beneficial owner (the natural person who owns or controls the legal persons and arrangements)
c) Understanding and, as appropriate, obtaining information on the purpose and nature of the business relationship
d) Conducting on-going due diligence on the business relationship and scrutiny of transactions undertaken through the course of that relationship to ensure that the transactions being conducted are consistent with your knowledge of the customer, their business and risk profile, including where necessary source of funds.

THIRD PARTY DETERMINATION

You shall take reasonable measures to determine whether the individual is acting on behalf of another person.

In cases where a third party is involved, you should take reasonable measures to establish the true identity about the third party and their relationship with the individual or entity on whose behalf the transaction is being conducted.

ENHANCED DUE DILIGENCE

You shall apply enhanced due diligence measures to persons and entities that present a higher risk (based on your risk assessment). Enhanced due diligence measures can include, but are not limited to:

a) Obtaining further information that may assist in establishing the customer's identity
b) Applying extra measures to verify the documents supplied
c) Obtaining senior management approval for the new business relationship or transaction
d) Establishing the person's or entity's source of funds
e) Carrying out enhanced on-going monitoring of the business relationship.

POLITICALLY EXPOSED PERSONS (PEPs)

You shall have appropriate risk management systems to determine whether your customer and beneficial owner is a politically exposed person (PEP). You shall take the following measures where a customer or beneficial owner is a politically exposed person, a family member or a close associate of a PEP.

For foreign PEPs and high-risk business relationships with a domestic or international organization PEP:

a) Obtaining senior management approval to transact or establish the relationship
b) Take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or transactions
c) Conduct on-going monitoring of the relationship.

RECORD KEEPING

You shall ensure that you maintain and keep records of all transactions and customer due diligence measures for a minimum period of 7 years from the date the relevant business or transaction was completed or following the termination of an account or business relationship.

NEW TECHNOLOGIES

You shall take reasonable measures to prevent the use of new technologies for money laundering and terrorism financing purposes by conducting and documenting a money laundering and terrorism financing risk assessment prior to the introduction of a new product, business practice or delivery method. A risk assessment should also be conducted when considering the use of new or developing technologies for both new and pre-existing products.

Additional information on how to comply with these obligations can be found on the Registrar of Company's Website <companies.govmu.org>. This includes on the Measures for the Prevention of Money Laundering and Countering the Financing of Terrorism in the Company and Service Provider Sector [*companies.govmu.org*]. Also, an AML/CFT Guidance on Suspicious Transaction Reports has been prepared by the Financial Intelligence Unit:

http://www.fiumauritius.org/English/Reporting/Documents/Guidance%20Note_310817.pdf.