Risk Management Insurance Brokerage Ltd (RMIB)

Policy Statement On

Anti-Money Laundering and Counter-Terrorist Financing

(1) Culture and Values

RMIB takes all reasonable measures to ensure that proper safeguards exist:

- to mitigate the risks of Money Laundering (ML) and Terrorist Financing (TF) and
- to prevent a contravention of any requirement under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap.615) ("the AMLO"), and the most current Guideline on Anti-Money Laundering and Counter-Terrorist Financing (AML Guideline).

RMIB establishes and implements adequate and appropriate Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) policies, procedures and controls, taking into account factors including types of customers, products and services offered, delivery channels and geographical locations involved.

(2) Allocation of Responsibilities

RMIB's senior management undertakes its assessment of the risks the firm faces and how the ML/TF risks are managed and ensure all relevant staff are trained and made aware of the law and their obligations under it.

To adequately manage ML/TF risks, RMIB appoints a Compliance Officer (CO) (named Tong Kar Yee) to act as a focal point for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management.

RMIB appoints a Money Laundering Reporting Officer (MLRO) (named Danny H Yao - Director) as a central reference point for reporting suspicious transactions to the Joint Financial Intelligence Unit of the Hong Kong Police Force. The MLRO receives full cooperation from all staff and full access to all relevant documentation enabling him/her to perform his/her functions.

RMIB adopts appropriate measures to let frontline staff know the responsible areas and judge whether a transaction is suspicious and report them promptly to CO or MLRO."

(3) Risk Identification and Assessment

RMIB applies a risk-based approach to assess which customers are at a higher risk of ML/TF. The followings are some risk factors to be identified:

1. types of customers and behavior;
2. if the customer is a Politically Exposed Person (PEP) or has ties to known terrorist organizations
3. products and services offered; (see Appendix)
4. delivery channels; and
5. customer's business organization/geographical locations involved

RMIB takes enhanced measures (including customer due diligence and ongoing monitoring) to manage those customers with higher risks and apply simplified rules to customers with lower risks.

(4) Customer Due Diligence (CDD), Record Keeping and Ongoing Monitoring

RMIB will apply the CDD measures, as stated in the AML Guideline Chapter 4.

RMIB adopts a risk-based approach to implement appropriate controls and oversight and to determine the extent of due diligence to perform and the level of ongoing monitoring to be applied.

RMIB will monitor the business relationship with our customers under the conditions stated in the AML Guideline Chapter 5.

RMIB will keep the documents obtained in the course of identifying and verifying the identity of the customer and maintain the documents obtained in connection with the transactions for five (5) years after the end of the business relationship or the date of the occasional transaction.

(5) Staff Awareness to AML/CFT

All relevant staff (including new staff) will receive proper training, either through in-house training or through appropriate seminars provided by relevant authorities to ensure they are made aware of the AMLO and to recognize suspicious ML/TF activities/transactions.

RMIB will keep training records/records of relevant courses or seminars attended for inspection by the regulator.

(6) Reporting Suspicious Activities/Transactions

RMIB will give all relevant staff sufficient guidance to enable them to take appropriate actions when detecting suspicious transactions and report suspicious activities/transactions to CO / MLRO as soon as possible. Details of reporting methods and advice are on the website of the Joint Financial Intelligence Unit.

Where exceptional circumstances exist concerning an urgent disclosure, we will make an initial notification by telephone to the local police.

(7) Internal Monitoring System

RMIB carries out regular assessments of the adequacy of our systems and controls to ensure that we manage the ML and TF risks effectively and are compliant with the AMLO and the AML Guideline.

(8) Regular Review

RMIB keeps the policies and procedures under regular review and assesses that the risk mitigation procedures and controls are working effectively.

Others

(9) Personal Data (Privacy) Ordinance

According to the Personal Data (Privacy) Ordinance, Chapter 486, RMIB shall protect the privacy of the customer/individual concerning personal data and shall use the personal data for which they were initially collected or a directly related purpose unless the data subject has given prior consent.

(10) Cooperation with Regulator and Law Enforcement Agencies

RMIB shall cooperate with the Customs & Excise Department about their routine inspection or investigation. RMIB will also assist with other law enforcement agencies wherever required under the laws of Hong Kong.

RMIB shall implement the above policies, procedures, and controls to mitigate the risks of money laundering and terrorist financing.

Appendix

I. Policies Requiring Approval and Enhanced CDD

The following long terms insurance contracts are considered vulnerable as a vehicle for laundering money or financing terrorism:

a) unit-linked or high profile single premium contracts;
b) single premium life insurance policies that store cash value;
c) fixed and variable annuities; and
d) (second hand) endowment policies

Ensure Mainland Chinese Visitors (MCV) sign The Important Facts Statement when purchasing long term insurance contracts.

The CO and MLRO must approve all the above policies before placing with the relevant insurer, and enhanced CDD must be performed and properly recorded.

The list is not exhaustive and is subject to amendment when needed.