2022

AML-CFT AND KYC PROCEDURES & POLICY

EASY WAY GLOBAL LIMITED

Unit Level 12F(1), Main Office Tower, Financial Park Labuan, Jalan Merdeka, 87000 Federal Territory of Labuan, Malaysia

Table of Content

1. INTRODUCTION

a. Purpose

i. This Document is Compilation of Anti Money Laundering and Counter Financing of Terrorism (AML-CFT) policies and procedures of the **"Easy Way Global Limited"** in order to comply with the guidelines of *Anti-Money Laundering, Anti-terrorism Financing Act 2001 (AMLATFA)* and perform the *Financial Action Task Force's* (FATF) 40 recommendation. It is intended to ensure that the **"Easy Way Global Limited"** understand and comply with requirements and responsibilities essential to them.

ii. The **"Easy Way Global Limited"** will not permit the use of Brokerage service for Money Laundering and Terrorist Financing Purposes.

iii. This document is also framed to ensure that all employees, IBs, and all affiliates understand and comply with the requirements and responsibilities essential to them.

iv. Training and education purposes.

b. Legal Provision

These guidelines are issued pursuant to:

2. WHAT IS MONEY LAUNDERING

a. **Definition**

Money laundering is a process of concealing the true origin and ownership of illegally obtained money. Principally, it is proceeds of criminal activities such as illicit drugs, corruption, organized crime, fraud, sex trade, forgery, illegal logging/fishing, revenue evasion, counterfeit money, piracy, terrorism, etc. which criminals attempt to disguise.

b. **Money Laundering Process**

There is more than one method of laundering money. Methods can range from purchase and resale of real estate or a luxury item to passing money through a complex web of legitimate businesses and 'shell' companies. In most cases, the proceeds of these criminal activities take the form of cash. There are three stages of money laundering, during which there may be numerous transactions made by launderers that could alert us.

c. **Placement – First Stage**

Placement is the physical disposal of the cash or asset derived from illegal activity. It includes the opening of numerous bank accounts, depositing cash, exporting cash, and using cash to purchase high-value goods such as property or businesses.

d. **Layering- Second Stage**

Layering is the separation of criminal proceeds from their source by creating a complex layering process of financial transactions designed to defeat the audit trail and provide anonymity. It may include telegraphically transferring funds overseas, depositing cash overseas, reselling goods previously with cash.

e. **Integration-Third Stage**

The integration provides apparent legitimacy to criminally derived wealth. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. This may be achieved through a complex web of transfers or income from apparently legitimate businesses previously purchased with the proceeds of illegal activities.

f. **Examples**

Examples of the types of transactions that are associated with money laundering and terrorist financing activities are documented in the **Appendix.** These are by no means exhaustive but are given as an indication of the type of activity involved.

3. WHAT IS FINANCING OF TERRORISM

Terrorist financing involves collecting and providing funds for terrorist activity. The primary objective of terrorism is 'to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act'.

The goal of the terrorist or terrorist organization is to maintain financial support in order to achieve their aims, and a successful terrorist group is one that is able to build and maintain an effective financial infrastructure. Terrorist needs finance for a wide variety of purpose – recruitment, training, travel, materials and setting up safe havens. Terrorist control funds from a variety of sources around the world and employ sophisticated techniques to move funds between jurisdictions. In order not to be detected, a terrorist group draws in the service of banks and non-banking institutions and takes advantage of their services products.

3.1 Financing Terrorism and Associated activities

If a known terrorist organization conducts or seeks to conduct a transaction via the business (whether or not the transaction or proposed transaction involves cash), such transaction or proposed transaction is deemed to be a suspicious transaction and the business must submit a report to the Supervision & Monitoring Unit of Labuan Financial Services Authority ("Labuan FSA") (refer **Appendix)**.

4. OUR POLICY AND FRAMEWORK

a. DUTY OF VIGILANCE

We are expected by the Anti-Money Laundering and Anti-Terrorism Financing Act and the Labuan FSA to have in place adequate policies, practices, and procedures that promote high ethical and professional standards and prevent the institution from being used, intentionally or unintentionally, by money launderers and terrorist financiers. The policies and procedures in this manual implement the duty of vigilance expected of us to avoid assisting the process of laundering and terrorist financing and to react to possible attempts at being used for those purposes. AML policies approved by the Board of Directors of Easy Way Global Limited and that any amendment or revision made or to be made to the AML/CTF Policy shall be done with prior approval of the Board and in accordance with the internal procedures governing Easy Way Global Limited

b. PRINCIPLES

- We oppose the crimes of money laundering and terrorism financing and do not tolerate the use of our products and services for either of these purposes.
- We are committed to playing our role in the fight against money laundering and terrorism financing.
- We will comply with the letter and the spirit of the laws and regulations of the Labuan FSA that relate to Anti-Money Laundering and Countering Financing of Terrorism.
- We will provide our products and services only for legitimate purposes to persons whose identities we have been able to reasonably ascertain.
- We will halt and report to the regulatory any relationships with those that we reasonably assess as representing too high a risk of money laundering or terrorism financing.
- We will help our staff manage the issues that might arise for them when dealing with people they know, including kin.
- Our owners, management, and staff will be treated in the same way as all other applicants when they apply to use our services.
- We report any activity that we detect which we regard as suspicious to the Anti-Money Laundering Compliance Unit of Labuan FSA.
- Our staff will receive the Anti-Money Laundering and Countering Financing of Terrorism training they need to understand their obligations under the law and to perform in their roles.
- We will monitor our customers, their transactions, and our people, consistent with the level of money laundering and terrorism financing risk they represent.
- We will comply with the requirement of Anti-Money Laundering Compliance Unit of Labuan FSA and inform them of any material changes that may occur within our business at any time.
- Our office will adhere to the requirements as per guidelines of Labuan FSA on the appointment of or update on any changes regarding our Compliance Officer.
- We are aware that our owners, management and staff are subject to a fit and proper screening by Labuan FSA and could be removed as a disqualified person within the meaning Labuan FSA guidelines.

c. OUR Anti-Money Laundering and Countering Financing of Terrorism (AML & CFT) PROGRAM

Our AML & CTF Program is made up of the contents of this manual. Our activities can be described as a series of controls to manage the way we:

- accept applications for transactions;
- monitor the transactions we do for unusual activity that needs further investigation;
- identify events that require us to take further action;
- report certain matters to Anti-Money Laundering Compliance Unit of Labuan FSA; and
- Keep records of what we do.

Some of the controls we will use are embedded in the way our products operate

d. DISCIPLINARY ACTION AND DISMISSAL

- Our staff will face disciplinary action, and possibly dismissal, if they fail to follow the AML & CTF procedures and requirements in this manual. We will dismiss any person who is involved in facilitating money laundering, terrorism financing or who launders money or finances terrorism using our products and services, and we will comply with any law that requires us to report such matters to Labuan FSA and law enforcement. Law enforcement receives our full cooperation in the prosecution of such matters against our staff.

- Sometimes customers or transactions involve people we know well or may involve the owners of this business or someone else close to us. Even if this is the case all our staff are still expected to follow the procedures in this manual.

- Staff should go to the “Compliance Officer” if they are experiencing difficulties with this area.

e. FRAMEWORK

The concept of customer due diligence in the organization can be achieved through a set of transparent clear policies, and procedures to guide staff of the company to implement and enforce effective anti-money laundering measures. These measures control to assist in securing a base of genuine clients and to generate long-term reputable business.

The company will conduct its business in compliance with the following components of the framework:

i. Customer Due Diligence.
ii. Verification.
iii. Record Keeping.
iv. Reporting.
v. On-Going Monitoring.
vi. Suspicious Transaction Monitoring/ Reporting.
vii. Training Program.

5. CUSTOMER DUE DILIGENCE

The purpose of verification is to establish that the brokerage service is a genuine transaction and this can be achieved by knowing your customers “KYC”. The concept of KYC is a critical precondition to recognize a suspicious or unusual transaction. It is through a series of facts confirmation during the verification that one buildup knowledge about his/her customers. Customer Due Diligence must be conducted and satisfactory evidence must be obtained. The identity and legal existence of any person applying to conduct business must be properly established.

a. WHEN IS CDD REQUIRED?

CDD is required when:

i. Establishing a business relation.
ii. It has any suspicion of ML/TF.

iii. It has any doubt about the accuracy or adequacy of previously obtained information.

b. WHAT IS REQUIRED?

i. Identify the customer and verify that customer's identity using reliable, legitimate source documents, data or information. For Example: Copy of any Government ID for Identification and a copy of Utility Bill for Address Verification.

ii. Verify that any person purporting to act on behalf of the customer is so authorized and identify and verify the identity of that person.

iii. Understand, and where relevant, obtain information on, the purpose and intended nature of the business relationship.

iv. To verify that the fund transferred to the customer is to the customer's own account.

v. Sight the original identification documents (stamping of **True Copy of ID verified** from Original) of all customers, regardless of the amount transacted.

6. PRECISE CUSTOMER DUE DILIGENCE

A. INDIVIDUAL CUSTOMER

i. In conducting CDD on an Individual customer, the following information is at least required to be obtained:

- Full Name
- Passport Number and country of issuance
- Residential and Mailing Address Proof
- Date of Birth
- Nationality
- Occupation Type
- Name of employer or nature of self-employment/nature of business
- Source of Fund
- Home, Work and Mobile Contact Number

ii. Verification of the documents requires the customer to furnish the original document, make a copy of the said document. Whereby biometric identification method is used, verification is deemed to be satisfied.

iii. Where there is any doubt, the customer is required to produce other supporting official identification documents bearing their photograph, issues by an official authority or an international organization to enable their identity to be ascertained and verified.

B. CORPORATE CUSTOMER

In conducting CDD on corporate customer, documents are required to identify, confirm its existence, good standing and authority of persons acting on its behalf. Documents required include:

a. Certificate of Incorporation
b. Shares Certificate
c. Certificate of Incumbency
d. Memorandum and Article of Association
e. Identity Proof of each shareholder, director and beneficial owner
f. Address proof of each shareholder, director and beneficial owner
g. Business License

C. **<u>POLITICALLY EXPOSED CUSTOMER (PEP)</u>**

- The company is required to put in place a risk management system to determine whether a customer is a foreign PEP.
- Upon determination that a customer is a foreign PEP, the requirements of enhanced CDD must be conducted.
- The company may apply CDD measures similar to other countries for PEPs if the company is satisfied that the PEPs are not assessed as higher risk.

D. **<u>NON-FACE TO FACE BUSINESS</u>**

- Appropriate measures for customer verification must established for non-face to face customers and implement monitoring and reporting mechanisms to identify potential money laundering and finance of terrorism activities.
- Special attention should be given in establishing and conducting business relationship via information communication technology which includes but not limited to internet, post, fax or telephone.
- Any business relationship or transaction that avoids face to face contract without proper customer identification and verification may subject to abuse by money launderers and financiers of terrorism in gaining access to economic system.
- The measures that can be used in verifying the non-face to face customer may include but not limited to:
    a. Requisition of additional documents to complement those which are required for face to face customers
    b. Developing independent contact with customer
    c. Verification of customer information against database maintained by the authorities.

E. **<u>HIGHER RISK CUSTOMER</u>**

For Higher Risk Customer, enhanced due diligence must be conducted.

- The following are deemed as Higher Risk Customer:
    a. Individual Payment of USD 10,000 and above.
    b. Any cases based on the facts and circumstances with reasonable ground for suspecting a possible case of money laundering.
    c. High net worth individuals. - Supporting documents will be requested to verify the expected Turnovers of Transactions.
    d. From Location known for their high rates of crime (drug producing, trafficking, smuggling).
    e. Countries or jurisdiction with inadequate AML/CFT laws and regulations as highlighted by the FATF- High Risk Countries.
    f. Politically Exposed Person. – Screening of Name, ID verification to be done and Enhanced Due Diligence will be done.
    g. Business/activities identifies by the FATF as of higher money laundering and financing of terrorism risk.
- To complete and submit the High-Risk Customer Report.

F. **<u>HIGHER RISK COUNTRIES</u>**

a. The Company is required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF as having on-going or substantial ML/TF risks.

b. Where ML/TF risks are assessed as higher risk, the Company is required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

c. In addition to the enhanced CDD requirement, Company is required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries listed as having ongoing or substantial ML/TF risks, as follows:
    - Limit business relationship or financial transactions with identified countries or persons located in the country concerned;
    - Review and amend, or if necessary, terminate, correspondent banking relationships with financial institutions in the country concerned;
    - Conduct enhanced audit, by increasing the intensity and frequency, for branches and subsidiaries of the reporting institution or financial group, located in the country concerned;
    - Submit a report with a summary of exposure to customers and beneficial owners from the country concerned to the Financial Intelligence

List of High-risk Countries

- Afghanistan
- American Samoa
- The Bahamas
- Botswana
- Democratic People's Republic of Korea
- Ethiopia
- Ghana
- Guam
- Iran
- Iraq
- Libya
- Nigeria
- Pakistan
- Panama
- Puerto Rico
- Samoa
- Kingdom of Saudi Arabia
- Sri Lanka
- Syria
- Trinidad and Tobago
- Tunisia
- US Virgin Islands
- Yemen
- Serbia
- Israel

G. RELIANCE ON THIRD PARTIES

- On Going Customer Due Diligence (CDD)

a. The Company may rely on third parties to conduct customer due diligence and introduce business.

b. The ultimate responsibility and accountability of CDD measures shall remain with the company relying on the third parties.

c. The Company must be satisfying that the third party at the minimum:
    - Can obtain immediately the necessary information concerning CDD.
    - Has an adequate customer due diligence process
    - Has measures in place for record keeping requirements
    - Can provide the CDD information and copies of the relevant documentation immediately upon request.
    - Is properly regulated and supervised by the respective authorities.

d. The company may obtain an attestation or written confirmation from the third party that they have conducted the CDD on the customer and bank account holder.

- On Going Customer Due Diligence (CDD)
  The company shall not rely on third parties to conduct on-going due diligence exercise.

H. REFERRED LIST

a. Prior to accepting customers, their names will be checked against the referred list. The Company will not establish or maintain a relationship with any person, entity or group designated on any of the following referred lists:

   The United Nation Sanctions List

   FATF High Risk List.

   List of PEPs.

b. No PEPs should be accepted except for PEPs, where cases involved PEPs approval to be obtained from Senior Management before acceptance of the business.

c. Internal Suspicious Transaction Reporting (ISTR) form shall be generated and escalated for review to the Compliance Officer in the event of a match against the referred risk.

d. The Compliance Officer will take the necessary action and subsequently report to the regulators, where necessary.

I. ENHANCED DUE DILIGENCE

- Enhanced Due Diligence is conducted where the ML/TF risks are assessed as higher risk and should include the following:
  a. Obtaining CDD information under verification process for individual customer and beneficial owner;
  b. Obtaining additional information on the customer and beneficial owner (e.g., volume of assets and other information from public database);
  c. Inquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and
  d. Obtaining approval from the Senior Management of the reporting institution before establishing (or continuing, for existing customer) such business relationship with the customer. In case of PEPs, Senior Management refers to the Senior Management at the Head office.

- The Company may also consider the following enhanced CDD measures in line with the ML/TF risks identified:
  a. Obtain additional information on the beneficial owner of the beneficiaries (for example occupation, volume of assets, information available through public databases or internet); and
  b. Requiring the first payment to be carried out through an account in the beneficial owner's name with a financial institution subject to similar CDD measures.
- Practice of Enhanced Customer Due Diligence Form – (Refer Appendix 6)

Note: The Account holder/beneficial account shall be hold by the customer him/herself.

J. ONGOING DUE DILIGENCE

- The relevant departments should take the necessary measures to ensure that the records of the existing customers, including its customer profile are relevant and remain updated.
- Regular review must be conducted on existing records of customers especially:
  a. Scrutinizing transaction undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, their business and risk profile, including where necessary, the source of funds.
  b. Ensuring that documents, data or information collected under the CDD process is kept up to date and relevant, by undertaking reviews of existing records particularly of higher risk customers.
  c. Since most detection would be made through analyzing the transaction patterns or activities of the customer at the point of customer contact the following types of transaction should be monitored:
     - Appears Unusual.
     - Is inconsistent with the expected type of activity and business model when compared to the volume of transaction.

- Does not have any apparent economic purpose.
- Cast doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customers.

- The frequency of the on-going due diligence and enhanced diligence shall commensurate with the level of ML/TF risk posed by the customer based on the risk profiles and nature of transactions.

7. FAILURE TO COMPLETE SATISFACTORILY CUSTOMER DUE DILIGENCE

- The respective business department should not commence business relations or perform any transaction in relation to a potential customer or shall terminate business relations on the case of an existing customer, if company is unable to comply with the customer due diligence requirements.
- In the case of existing business relations with customers, it should terminate such business relations if the customer fails to comply with the customer due diligence requirements.

8. SUSPICIOUS MONEY LAUNDERING TRANSACTION REPORT

- *The Company is required to promptly submit a suspicious report to the Financial Intelligence Unit whenever the reporting institution suspects or have reasons to suspect that the transaction (including attempted or proposed), regardless of the amount:*
  - *Appears unusual;*
  - *Has no clear economic purpose;*
  - *appears illegal;*
  - *Involves proceeds from an unlawful activity; or*
  - *Indicates that the customer is involved in ML/TF*

- *The Company must provide the required and relevant information that gave rise to doubt in the suspicious transaction report form, which includes but is not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.*

- *The Company must establish a reporting system for the submission of suspicious transaction reports.*

- *suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and to Anti-Money Laundering Compliance Unit, Labuan Financial Services Authority whenever the reporting institution suspect or have reason to suspect that the transaction (including attempted or proposed), regardless of the amount:*
  - *appears unusual;*
  - *(b) has no clear economic purpose;*
  - *(c) appears illegal;*
  - *(d) involves proceeds from an unlawful activity; or*
  - *(e) indicates that the customer is involved in ML/TF.*
- *Triggering of Red Flags*

  Easy Way Global Limited will look for "red flags" relating to:
  - *Location of the business*
  - *Occupation or nature of business*
  - *Purpose of the business transactions*
  - *Expected pattern of activity in terms of transaction types, volume, and frequency*
  - *Expected origination of payments and method of payment*
  - *Articles of incorporation, partnership agreements and business certificates*
  - *Understanding of the customer's customers (KYCC)*
  - *Identification of beneficial owners of an account or customer*
  - *Details of other personal and business relationships the customer maintains*
  - *Approximate salary or annual sales*
  - *AML policies and procedures in place*
  - *Third-party documentation*
  - *Local market reputation through review of media sources*

- *STR Reporting - The Compliance Officer will submit the suspicious transaction report in the specified suspicious transaction report form through the following modes: Mail:*

Director
Financial Intelligence and Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)
Fax: +603-2693 3625
Email: str@bnm.gov.my

AND

Director
Supervision and Monitoring Unit
Labuan Financial Services Authority
Level 17, Main Office Tower
Financial Park Complex
Jalan Merdeka
87000 Labuan F.T.
Attention to: Anti-Money Laundering
Compliance Unit
(To be opened by addressee only)
Fax: +6087-453442
Email: aml@labuanfsa.gov.my

9. REPORT KEEPING POLICY

- The Company is required to keep the relevant records including any accounts, files, business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the identity of customers and results of any analysis undertaken. The records maintained must remain up-to-date and relevant.
- The Company is required to keep the records for at least six years following the completion of the transaction of the termination of the business relationship.
- In situations where the records are subjected to on-going investigation or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the relevant law enforcement agency that such records are no longer required.
- The Company is required to retain the relevant records in a form that is admissible as evidence in court and make such available to the supervisory authorities and law enforcement agencies in a timely manner.

Note: All suspicious transaction shall be submitted to Board of Directors/ Senior Management on the same day and to the Financial Intelligence Unit the next working day.

10. COMPLIANCE OFFICER

Who is our Money Laundering Compliance Officer?

Name: TBA

Contact detail: compliance@easywayglobalfx.com

11. ROLES AND RESPONSIBILITIES

Board of Directors (BOD) & Senior Management

- Members of Board of Directors (Board Members) shall understand their roles and responsibilities in managing ML/TF risks faced by the company.
- Board members must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services.
- Board members must understand the AML/CFT measures required by the laws including the AMLATFA, subsidiary legislation and instruments issued under the AMLATFA, and the industry's standards and best practices as well as the importance of implementing AML/CFT measures to prevent the reporting institution.

The BOD has the following roles and responsibilities:

- Maintain accountability and oversight for establishing AML/CFT policies and minimum standards;
- Approve policies regarding AML/CFT measures within the company, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;
- Establish appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the company's products and services, technology as well as trend in ML/TF;
- Establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the company;
- Define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;
- Ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;
- Assess the implementation of the approved AML/CFT policies through regular reporting and updates by the Senior Management and Audit Committee; and
- Establish MIS that is reflective of the nature of the company's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.
- Inclusion of to inform, in writing, the Labuan Financial Services Authority within ten working days on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as maybe required by Labuan Financial Services Authority.

Compliance Officer:

The Compliance Officer is a senior staff member reporting to Managing Director and is responsible for:

- Creating and keeping this manual current;
- Monitoring the compliance by our business with the requirements of the laws and regulations of the Labuan FSA that relate to AML & CTF;
- Monitoring transactions undertaken for Customers;
- Identification and management of money laundering risk using our services;
- Providing leadership and training on AML & CTF issues to our staff, including new staff;
- Acting as the liaison point with the Labuan FIU;
- Investigating unusual matters and reporting those that are suspicious to our Labuan FIU;
- Reporting all other matters that must be reported to the Labuan FIU;
- Ensuring that our staff know what their responsibilities are;
- Monitoring employees in the course of performance of their duties;
- Ensuring that our staff are aware of the requirements of this manual and of the AML & CTF laws and regulations that apply to our business;
- Helping our staff where they face problems associated with Customers who they know well or who are kin;
- Overseeing corrective actions where gaps are identified in our operations with the procedures in this manual;
- Compliance Officer are clearly defined and documented with a more detailed and comprehensive job description (JD) which will describe the functions, requirement and the responsibilities of Easy Way Global Limited
- Reviewing this manual periodically for its adequacy;

- Arranging for periodic independent review of this man.

12. EMPLOYEE TRAINING AND AWARENESS PROGRAMME

- The effectiveness of the vigilance system depends on the extent to which the staff members comprehend the issues surrounding money laundering and terrorism financing and their respective obligations under the AML/CFT Framework, as well as their obligations to comply with both the guidelines and any relevant legislation.
- The awareness and training programs on AML/CFT practices and measures are mandatory for the following level of employees:
  a. New Employees
  b. Sales Executives
  c. Dealers
  d. Supervisors and Managers
- Senior Management must ensure that a proper channel of communication is in place to effectively communicate to all levels of staff, the AML/CFT policies and procedures. All staff members should be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements
- Compliance Unit must make available its AML/CFT measures for all staff members and its documented AML/CFT procedures containing the following:
  a. Internal AML/CFT policies and procedures.
- Training conducted for employees must be appropriate to their level of responsibilities in detecting ML/FT activities and the risk faced by the company. All new frontline employees are required to complete initial AML/CFT training upon joining.
- Training for all employees may provide a general background on ML/TF, the requirements and obligations to monitor and report suspicious transactions to the Money Laundering Reporting Officer and the importance of CDD and the Suspicious Transaction Report (STR) procedures. Employees dealing with the customers.
- Training Records
  a. The HR Department must maintain records of all formal training provided to the employees.
  b. The Compliance Department shall also retain records for the training provided to and attended by the relevant employees.
  c. These records shall include the names of attendees and dates of the training and shall be readily available for review.

13. SCREENING PROCEDURE

- This applies to all new and existing employees and agents.
- All On board Customers names will be Screened via OFAC Treasury (https://sanctionssearch.ofac.treas.gov/)
- Easy Way Global Limited will do the necessary verification to ensure that the customer is not listed in the United Nations Security Council Resolution (UNSCR 1267) list of terrorist where there are existing sanctions against individual and entities related to, The updated and consolidated United Nations List can be obtained at (https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list)
- The Screening procedures shall apply before the employee or agent sign the respective employment or agency contract and throughout the course of employment or agency.
- The assessment shall include an evaluation of the following:
  - Employee/Agent Personal Information.
  - Employment/Agent History
  - Employee/Agent Financial History
  - Employee/Agent Criminal Records

14. COMPLIANCE AND AUDIT FUNCTION

- The board is required to ensure that the roles and responsibilities of the auditors are clearly defined and documented and at a minimum should include:
  a. Checking and testing the compliance with and effectiveness of the AML/CFT policies, procedures and controls.
  b. Assessing whether the current measures are in the line with the latest developments and changes to the relevant AML/CFT requirements.

- The scope of the independent audit shall include at a minimum:
  a. Compliance with AMLAFTA, its subsidiary legislation and instruments issued under the AMLATFA.
  b. Compliance with the reporting institution’s internal AML/CFT policies and procedures

c. Adequacy and effectiveness of the AML/CFT compliance program.
d. Reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

- The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of AML/CFT measures and any inadequacy in internal controls and procedures.

- The company is required to ensure that independent audits are carried out at least on an annual basis.

15. INTERNAL REPORTING

- Employees must report any relevant money laundering suspicions to the compliance officer.
- The suspicion should be fully documented, including the name and location of the reporting employee, full details of the client and the respective account, description of the information giving rise to the suspicion.
- The Compliance officer should remind the reporting employee to avoid "tipping off" the subject of the reported suspicion, and that information concerning a report should not be disclosed to any third parties.

16. EXTERNAL REPORTING

Compliance Officer or his duly authorized delegate will consider the reported information, and where, following consideration, the suspicion remains, a report must be made to "Anti-Money Laundering Compliance Unit" of Labuan FSA.

In order to make this assessment, the compliance officer will have to assess information, including "know your business" in the company's possession that could be relevant. Know your business information will include: information about the financial circumstances of a client or any person on behalf the client has been acting or is acting; and features of the transactions which the company has entered into with or for the client.

APPENDIX-1

INTERNAL SUSPICIOUS TRANSACTION REPORT FORM

DETAILS OF REPORTING DEPARTMENT & BRANCH			
(Customer will not be informed/alerted on the reported case)			
1	Date		
2	Department		
3	Name of the Reporter		
4	Contact Details		
5	Purpose of Reporting		
DETAILS OF THE CUSTOMER			
INDIVIDUAL			
1	Nationality		
2	Name		
3	Other/Previous Name	a.	
		b.	
		c.	
4	New Identity Number		
5	Other Identification		
6	Other Identification Type		
7	Gender		
CONTACT INFORMATION			
1	Residential/Business Address		
2	Correspondance Address		
3	Other Address		
4	Previous Address		
5	Email Address		
6	Contact No. (Work)		
7	Contact No. (Residence)		
8	Contact No. (Mobile)		
9	Fax. No.		
EMPLOYMENT INFORMATION			
1	Business/Employment Type		
2	Occupation		
3	Occupation Description		
4	Employer Name		
5	Employment Area		
6	Other known Employment		
MARITAL INFORMATION			
1	Marital Status		
2	Spouse Name		
SPOUSE IDENTIFICATION			
1	New NRIC No.		
2	Old NRIC No.		
3	Other Identification		
4	Other Identification Type		
5	Passport No.		
6	Place/Country of Issue		

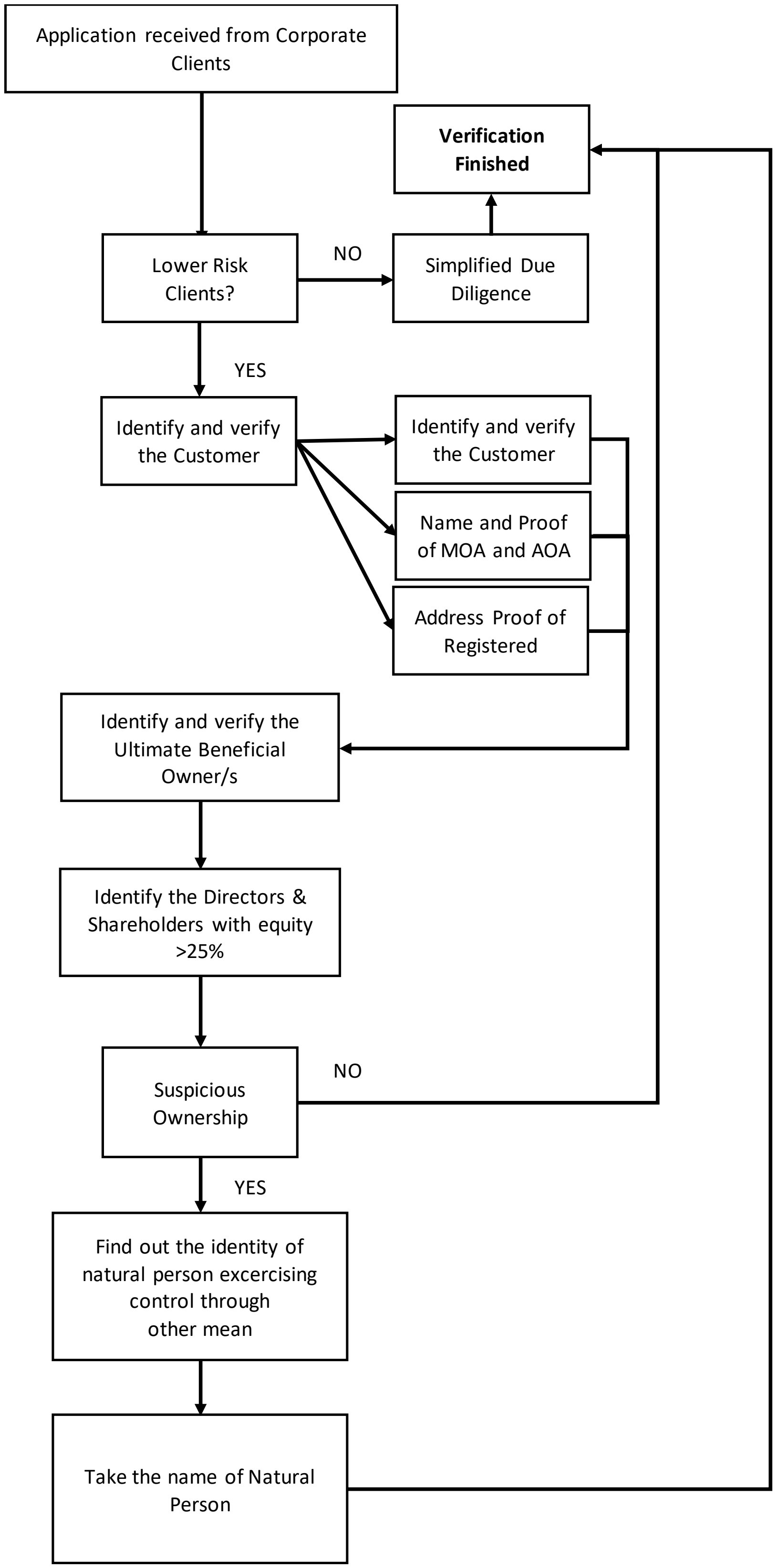
APPENDIX-2
HIGH RISK CUSTOMER REPORT

HIGH RISK CUSTOMER REPORT (HRCR)		
1	Name of Customer	
2	Passport No.	
3	Occupation	
4	Annual Income	
5	Description of Findings	
6	Review of Executive	
	Name of Executive	
	Designation	
	Date	
	Signature	
7	Review of Compliance Officer	
	Name of Complaiance Officer	
	Designation	
	Date	
	Signature	
7	Review of Board	
	Name	
	Designation	
	Date	
	Signature	

APPENDIX-3
HIGH RISK BUSINESSES

1. Remittance Agents
2. Money Changer
3. Casinos & Other Gambling Establishments
4. Nightclubs/ disco/ karaoke center
5. Massage Parlor
6. Travel Agencies
7. Import/Export Companies
8. Pawn Shop
9. Jewel/Gem/Precious metal dealers
10. Antique
11. Charity or Society with cross border donations
12. Off Shore Banks (Incorporated in non FATF member)
13. Off Shore Trust (Incorporated in non FATF member)
14. Multi-Level Marketing Business
15. Unlicensed Investment Company
16. Cash based business

APPENDIX-4
IDENTIFICATION AND VERIFICATION OF CORPORATE CLIENTS



APPENDIX-5

Examples of Suspicious Activities or Transactions associated with money laundering and terrorist financing

1. **Money Laundering using cash transactions**
    1. unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments;
    2. substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer;
    3. customers who deposit cash by means of numerous credits slips so that the total of each deposit is unremarkable, but the total of all the credits is significant;
    4. company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.);
    5. customers who constantly pay in or deposit cash to cover requests for money transfers, bankers' drafts or other negotiable and readily marketable money instruments;
    6. customers who seek to exchange large quantities of low denomination notes for those of higher denomination;
    7. frequent exchange of cash into other currencies;
    8. branches that have a great deal more cash transactions than usual (Head Office statistics detect aberrations in cash transactions);
    9. customers whose deposits contain counterfeit notes or forged instruments;
    10. customers transferring large sums of money to or from overseas locations with instruments for payment in cash; and
    11. large cash deposits using night safe facilities, thereby avoiding direct contact with bank staff.

2. **Money Laundering using bank accounts**
    1. customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominees;
    2. customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount;
    3. any individual or company whose account shows virtually no normal personal banking or business-related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account);
    4. reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify;
    5. customers who appear to have accounts with several institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds;
    6. matching of payments out with credits paid in cash on the same or previous day;
    7. paying in large third-party cheques endorsed in favor of the customer;
    8. large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
    9. customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions;
    10. greater use of safe deposit facilities and increased activity by individuals; the use of sealed packets deposited and withdrawn;
    11. companies' representatives avoiding contact with the branch;
    12. substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client, company and trust accounts;

13. customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable;
14. insufficient use of normal banking facilities (e.g. avoidance of high interest rate facilities for large balances); and
15. large number of individuals making payments into the same account without an adequate explanation.

3. **Money Laundering using investment related transactions**
    1. purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing;
    2. request by customers for investment management or administration services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing;
    3. large or unusual settlements of securities in cash form; and
    4. buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. **Money Laundering by offshore international activity**
    1. customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent;
    2. use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business;
    3. building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas;
    4. unexplained electronic fund transfers by customers, foreign currency drafts or other negotiable instruments to be issued;
    5. frequent requests for travelers' cheques or foreign currency drafts or other negotiable instruments to be issued; and
    6. frequent paying in of traveler's cheques or foreign currency drafts particularly if originating from overseas.

5. **Money Laundering involving financial institution employees and agents**
    1. changes in employee characteristics, (e.g. lavish lifestyles or avoiding taking holidays);
    2. changes in employee or agent performance, (e.g. the salesman selling products for cash has remarkable or unexpected increase in performance); and
    3. any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

6. **Money Laundering by secured and unsecured lending**
    1. customers who repay problem loans unexpectedly;
    2. request to borrow against assets held by the institution or a third party, where the origin of the assets in not known or the assets are inconsistent with the customer's standing; and
    3. request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to deal is unclear, particularly where property is involved.

7. **Sales and dealing staff**

    1. **New Business**

        Although long-standing customers may be laundering money through an investment business it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies.

        Investment may be direct with a local institution or indirect via an intermediary who "doesn't ask too many awkward questions", especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations will usually give rise to the need for additional enquiries:

a. a personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details;
b. a corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation;
c. a client with no discernible reason for using the firm's service, e.g. clients with distant addresses who could find the same services nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere; and
d. any transaction in which the counterparty to the transaction is unknown

e. **Intermediaries**

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and, depending on the designation of the account, preserving anonymity. Likewise, there are a number of legitimate reasons for dealing via intermediaries on a "numbered account" basis; however, this is also a useful tactic which may be used by the money launderer to delay, obscure or avoid detection.

Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.

f. **Dealing patterns & abnormal transactions**

The aim of the money launderer is to introduce as many layers as possible. This means that the money will pass through a number of sources and through a number of different persons or entities. Long-standing and apparently legitimate customer accounts may be used to launder money innocently, as a favor, or due to the exercise of undue pressure.

Examples of unusual dealing patterns and abnormal transactions may be as follows:

1. **Dealing patterns**
    1. A large number of security transactions across a number of jurisdictions;
    2. Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates;
    3. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request;
    4. Low grade securities purchased in an overseas jurisdiction, sold locally and high-grade securities purchased with the proceeds; and
    5. Bearer securities held outside a recognized custodial system.
2. **Abnormal transactions**
    1. a number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account;
    2. any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading; early cancellation, especially where cash had been tendered or the refund cheque is to a third party;
    3. transfer of investments to apparently unrelated third parties;
    4. transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices; and

5. other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries.

8. **Settlements**

1. **Payment**

Money launderers will often have substantial amounts of cash to dispose of and will use a variety of sources. Cash settlement through an independent financial adviser or broker may not in itself be suspicious; however, large or unusual settlements of securities deals in cash and settlements in cash to a large securities house will usually provide cause for further enquiry. Examples of unusual payment settlement may be as follows:

(i) a number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction;

(ii) large transaction settlement by cash; and

(iii) payment by way of cheque or money transfer where there is a variation between the account holder/signatory and the customer

2. **Registration and delivery**

Settlement by registration of securities in the name of an unverified third party should always prompt further enquiry.

Bearer securities, held outside a recognized custodial system, are extremely portable and anonymous instruments which may serve the purposes of the money launderer well. Their presentation in settlement or as collateral should therefore always prompt further enquiry as should the following:

(i) settlement to be made by way of bearer securities from outside a recognized clearing system; and

(ii) allotment letters for new issues in the name of persons other than the client.

3. **Disposition**

As previously stated, the aim of money launderers it to take "dirty" cash and turn it into "clean" spendable money or to pay for further shipments of drugs, etc. Many of those at the root of the underlying crime will be seeking to remove the money from the jurisdiction in which the cash has been received, with a view to its being received by those criminal elements for whom it is ultimately destined in a manner which cannot easily be traced.

The following situations should therefore give rise to further enquiries:

(i) payment to a third party without any apparent connection with the investor;

(ii) settlement either by registration or delivery of securities to be made to an unverified third party; and

(iii) abnormal settlement instructions, including payment to apparently unconnected parties.

9. **Company Formation and Management**

1. **Suspicious circumstances relating to the customer's behavior:**

(i) the purchase of companies which have no obvious commercial purpose;

(ii) sales invoice totals exceeding known value of goods;

(iii) customers who appear uninterested in legitimate tax avoidance schemes;

(iv) the customer pays over the odds or sells at an undervaluation;

(v) the customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, banker's drafts etc;

(vi) customers transferring large sums of money to or from overseas locations with instructions for payment in cash;

(vii) customers who have numerous bank accounts and pay amounts of cash into all those accounts which, if taken in total, amount to a large overall sum; and

(viii) paying into bank accounts large third-party cheques endorsed in favor of the customers.

2. **Potentially suspicious secrecy might involve**
   (i) excessive or unnecessary use of nominees;
   (ii) sales invoice totals exceeding known value of goods;
   (iii) performing "execution only" transactions;
   (iv) using a client account rather than paying for things directly;
   (v) use of mailing address;
   (vi) unwillingness to disclose the source of funds; and
   (vii) unwillingness to disclose identity of ultimate beneficial owners.

3. Suspicious circumstances in groups of companies:
   (i) subsidiaries which have no apparent purpose;
   (ii) companies which continuously make substantial losses;
   (iii) complex group structures without cause;
   (iv) uneconomic group structures for tax purposes;
   (v) frequent changes in shareholders and directors;
   (vi) unexplained transfers of significant sums through several bank accounts; and
   (vii) use of bank accounts in several currencies without reason.

APPENDIX-6

Enhanced Customer Due Diligence Form

Information collected in this form should be verified. Verification can be done subsequent to completing risk assessment.

Identification

FOR NATURAL PERSONS/SOLE PROPRIETORSHIPS ONLY			
Full legal name(s), both official and any aliases:		Unique identification number:	
Contact number(s):			
Nationality:			
Date of birth:			
Residential street address:			
Address of principal place of business (if different from above):			
Intended nature and purpose of the business relationship:			
Name of beneficial owner(s):			
Name of person(s) with executive authority:			

Additional Information required -

Question	**Response**	
Are you, or any party connected to you, a politically exposed person?	YES	NO
What country is your business based in?		
What type of products does your business sell or manufacture? Please provide further details in the box below if necessary.		
Any further Details		

Client/Agent's Declaration

I declare that the information provided in these forms is true and correct. I am aware that I may be subject to prosecution and criminal sanctions under written law if I am found to have made any false statement which I know to be false or which I do not believe to be true, or if I have intentionally suppressed any material fact.

Name of client/agent:	
Identity/passport number:	
Date:	
Signature:	

Verification (for office use)

Professional judgment will be exercised in determining if verification of identity should be that of "Normal CDD" or "Enhanced CDD" standards, depending on the risk assessment performed on the client.

For Normal CDD, the following documents can be used to verify the client's identity:

Copy of screening results from a reliable independent database (e.g. OFAC Treasury, United Nations List)	☐
Copy of passport or identification card	☐
A document containing the address of the individual (e.g., a bank statement or a recent utility bill)	☐

Notes:

1. None of the above factors on their own necessarily mean that a customer or other person is involved in money laundering. However, it may be that a combination of some of these factors could raise suspicions.
2. What does or does not give rise to a suspicion will depend on the particular circumstances.

Case Study

Placement

The very first bank to be prosecuted for failing to identify and to report deposits of illicit funds being deposited was a small bank in New York City. In that case, several different groups of people came into the bank on a regular basis and deposited cash, often just under the reporting thresholds. The people in each group would go up to separate tellers, and would frequently use different accounts, but it was fairly evident that they came into the bank together and were working together and that the accounts were related – the accounts having similar names.

One particular money launderer, Alfred Dauber, made regular cash deposits far in excess of the reporting thresholds into 12 different accounts and had the bank wire the funds to the country of Colombia. Dauber became the bank's largest customer and his cash deposits overwhelmed the tellers of the bank, but the bank was heedless of the risk or purpose of Mr. Dauber's accounts. It was estimated that Dauber made 250 deposits at the bank, totaling $46 million.

Overall, approximately $123 million was laundered through the bank by various people. The bank ended up pleading guilty to criminal charges and paying a criminal fine of $4 million.

Structuring

Structuring is perhaps the most well-known form of money laundering. It involves taking a large amount of cash and breaking it into smaller amounts so it can be deposited into financial institution without triggering reporting requirements.