Board Paper No :2023/595/11/N

Board Meeting No : 67 Date :27.11.2023

Lanka Credit and Business Finance PLC

ANTI-MONEY LAUNDERING

AND

COUNTERING THE FINANCING OF TERRORISM (AML/CFT) POLICY

Owner - Compliance Department
Approval – Board of Directors
Date of Approval – 27.11.2023

TABLE OF CONTENT

BY PARAGRAPH NUMBERS

1. INTRODUCTION

Lanka Credit and Business Finance PLC attaches the highest importance to prevent the company from being a utilized as a conduit and/or to be directly or indirectly be used for financial crime purpose/s by it's customers.

This policy is a high-level guide and sets out the relevant areas that employees of the company need to be aware of at all times. This Policy is issued to enable employees to obtain a general understanding on Anti Money Laundering/Terrorist Financing and should be read and understood in Conjunction with the other relevant and applicable circulars, instructions and guidance notes issued by the Compliance Unit from time to time.

Finance Companies are facing a heightened level of Anti Money Laundering and Prevention of Terrorist Financing Laws and Regulations due to the ever increasing threat of financial crime world wide. During the past several years, regulatory bodies have been aggressively stepping up their enforcement actions, and hence the financial industry is facing challenges in monitoring the adequacy of control methods utilized to prevent their Financial Institutions been used for such activities.

The Cost of Non-Compliance in very high and the resulted risk, such as the loss of reputation, penalties and monetary loss can be potentially fatal to any company.

In this Context, we at Lanka Credit and Business Finance PLC need to adopt strategies to deploy robust systems and adopt the highest level of Compliance. This is required not just to build a high level of trust amongst customers but also to maintain the confidence of customers, the Regulator and all other stakeholders.

Financial Institutions play a key role to combat the risks of money laundering and assist regulators in the fight against terrorist financing. It is the paramount duty and responsibility of the Company to know and understand its customers fully in terms of identity and activity to the extent of establishing the accuracy of its credentials in extending financial Facilities of any forms.

This exercise enables the company to identify adverse risks if any, associated with the applicant /customer (at the time of establishing an Entity relationship) and help guard against criminals/fraudsters making use of financing channels/services for their unlawful activities.

With the present day multi dimension delivery of financial services, channels and products, the need for a structured methodology for understanding customers at the time of establishing financial relationships and ongoing due diligence have assumed a greater importance.

Lanka Credit and Business Finance PLC (LCB Finance PLC) understand the Risks the Company is exposed to, and will periodically assess the risk through Compliance Risk Assessment (CRA) and include adequate controls and mitigations to our processes and systems from time to time.

a. SOME STEPS TAKEN AT LANKA CREDIT AND BUSINESS FINANCE PLC (LCB FINANCE PLC)

- Establishment of a Compliance Department under the Compliance Officer appointed at a senior management level who is dedicated to the task of overseeing LCB Finance's Compliance function and policies, practices and procedures with regard to Anti Money Laundering and Prevention of Terrorist Financing.

- Establishment of a Compliance Culture that values and rewards the implementation of appropriate Controls and Compliance procedures.

- Use of independent Compliance, Audit and Risk management Functions to help evaluate the Company's Compliance with applicable Anti Money Laundering laws, rules and regulations.

- The Company relies on those closest to our customers - The Branch Managers, the Front-line Staff, Sales staff etc. to fully understand with whom we are doing business and provide feedback whenever required.

- Conduct "Know Your Customer" (KYC) and ensure that the business we conduct on behalf of our customers is proper and in Compliance with applicable laws and Regulations.

- Continuous updating of policies and procedures to ensure that same meets or exceeds applicable norms in the financial Industry both locally and globally.

- The Company adopts a continuous Risk Based Framework methodology for assessment of Risk and Customer Due Diligence

1.2 THE COMPLIANCE STRUCTURE IN THE THREE LINES OF DEFENSE MODEL

Compliance Risk is the Risk arising due to non-Compliance with applicable Laws, Regulations and standards including Internal polices. Compliance risks could come in the form of Regulatory, legal, financial and reputational risk.

LCB Finance PLC employs a three line of defense mechanism in order to facilitate the management of Compliance Risk and is positioned as the second line of defense in the three lines of defense frame work of the company.

The Internal Audit Department as the third lines of defense whilst all Business/Operations/Services function as the first line.

2. INTRODUCTION TO RISK BASED COMPLIANCE

The Financial Intelligence Unit (FIU) of the Central Bank of Sri Lanka (CBSL) introduced the "Risk Based Approach" by way of CDD Gazette No 1951/13 of January 2016 and Circular No 1/18 with reference 037/05/002/0018/017 dated 11th January 2018.

The risk based approach starts with the identification and assessment of the risk to be managed with taking into consideration its customers, countries /geographical areas, products, services, transaction and delivery channels etc.

The intensity and extensiveness of risk management functions shall be in line with the "risk-based approach" and be proportionate to the nature, scale and complexity of the Company's activities, the customer profile and the money laundering and terrorist financing risk posed to the Company by way of it's day to day operations. The Company has already taken appropriate steps to identify, assess and manage its money laundering and terrorist financing risks in relation to its customers, based on countries or geographical areas, products, services, transactions and delivery channels.

3. DEFINITIONS

3.1 What is Money Laundering?

Definition of "Money Laundering"

"The process of converting cash or other property which is derived from criminal activity so as to give it the appearance of having been obtained from legitimate source" or "the act of concealing the transformation of profits from illegal activities and corruption into evidently "legitimate" assets"

The Process of Money Laundering

- There are, theoretically four factors that are common to Money Laundering operations:
- The real source of criminal money must be concealed and not be done without public knowledge.
- The form in which money is held must be changed in order to hide its identity.
- The trail of transaction must be obscured to defeat any attempted follow-up by law enforcement agencies.
- The launderer must maintain constant control on the monies as he cannot legally declare any theft/loss of such money.

Stages of Money Laundering Money Laundering

occurs in three (03) stages

Stage 1- Placement

This is the first movement of cash from it's source, as such placement means the consolidation and placement of different proceeds of criminal money in the financial system through different sources, or smuggling them out of the country. The objective of the launderer is to remove the proceeds of the illegal transaction to another location without detection and to transform them into transferable assets.

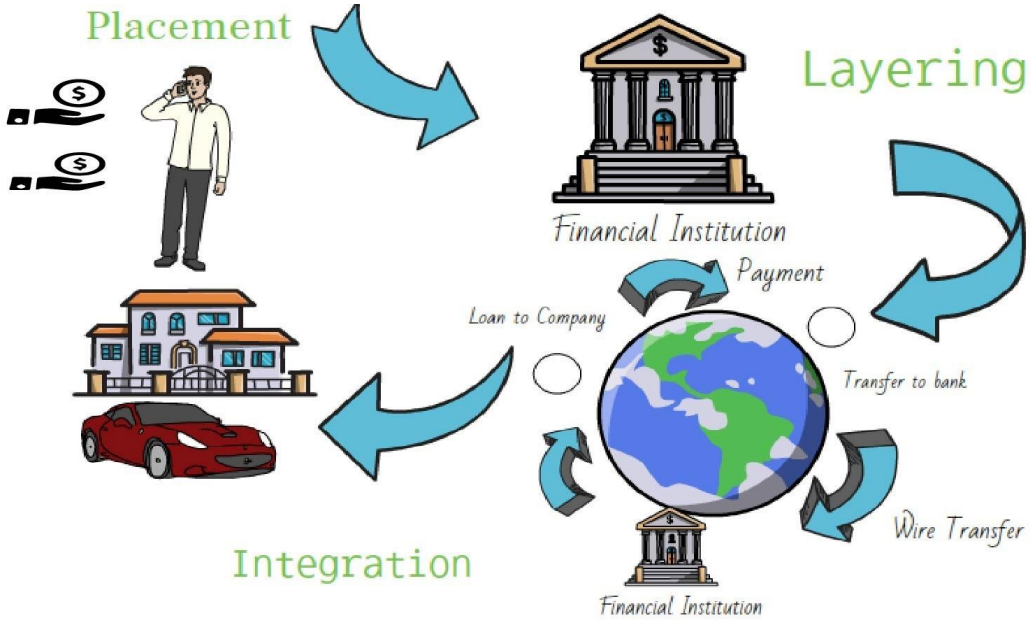
Stage 2 - Layering

The Launderer by moving the money through many accounts, through different countries and through dummy companies creates complex layers of transactions to disguise the trail and provide anonymity. This process will distance his deeds from his gains and obliterate the path of movement of funds.

Stage 3 – Integration

Once the money has been cleaned through the first two processes, "washed" or "cleaned "funds are brought back into circulation.

Example of a typical flow chart of Money Laundering



3.2 What is Terrorist Financing?

The United Nations International Convention for Suppression of Terrorist Financing defines Terrorist Financing in under mentioned manner in its Article-2 and also the recommendation of the Financial Action Task Force (FATF) gives the same definition. Most countries including Sri Lanka use this definition

Article 2

Any person commits an offence within the meaning of the Convention if that person by any means, directly or indirectly, unlawfully and willfully provides or collects funds or property with the intention that such funds or property should be used or in the knowledge that they are to be used or having reason to believe that they are likely to be used, in full or in part, in order to commit:

- an act which constitutes an offence within the scope of or within the definition of any one of the Treaties listed in the Convention on the Suppression of Terrorist Financing Act; or
- any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict or otherwise and the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an International Organization to do or to abstain from doing any act; or
- any terrorist acts

4. AML /CFT COMPLIANCE GOVERNANCE

4.1 Finance company Responsibilities in the Terms of Governance aspect

- Screening is to be conducted on all persons prior to been recruited by the Company and relevant document such as Police Report, Grama Sevaka Report, CRIB Reports Referral confirmation etc., as may be decided by the Finance companies Human Resource Department, in line with companies Recruitment policy is to be obtained.

- The Company shall appoint a dedicated Compliance Officer in terms of Section 1 4 of the FTRA, who shall be responsible for ensuring the Finance company's Compliance with the requirements of the relevant laws. This Officer will be at the senior management level in the organization structure of the Company and will be required to report to the Board Integrated Risk Management Committee.

- The Company to have an Internal Audit function to test all procedures and Systems from an independent aspect for Compliance as a third line of defence for the Company.

4.2 Board of Directors

Shall be Responsible for following

- Developing and maintaining an AML policy in line with evolving statutory and regulatory obligations.
- Ensure that the Company develops AML Compliance procedures on applicable regulations on combating Money Laundering/Terrorist Financing and ensuring that the staff keep up to date with new money laundering requirements and developments.
- Ensuring that staff are aware of their obligations in complying with the Company's policies and procedures.
- Ensure that staff are adequately trained in combating money laundering and Terrorist financing and a mechanism be established to communicate all relevant changes of related laws
- Seeking from the Compliance Division, at least annually, a report relating to the Company's Compliance with its Anti-Money Laundering obligations and a Compliance Risk Assessment.
- Ensuring that the Screening process is in place and carried out at the time of appointing or hiring of all employees whether permanent, contractual or outsourced.
- Appoint a senior management level Officer as the Compliance Officer who shall be responsible for ensuring the Financial Institution's Compliance with the requirements of the AML laws and rules and regulations.
- Ensure that the Compliance Officer or any other person authorized to assist him/her or act on his/her behalf, has prompt access to all customer records and other relevant information which may be required to discharge their functions

4.3 Compliance Officer (CO)

It is mandatory to appoint a Compliance Officer who shall be Responsible for ensuring the Institution's compliance with regulations relating to Anti Money Laundering and Prevention of

Terrorist Financing and to act on his/her own authority. The Compliance Officer would further co-ordinate matters with the Financial Intelligence Unit (FIU) of Central Bank of Sri Lanka (CBSL) and any Law Enforcement Authority accordingly.

The Compliance Officer appointed by the Company will be a Key Management Personnel (KMP) category staff member of the Company and required to obtain fit and proper certification from the Central Bank of Sri Lanka

Compliance Officer shall be Responsible For/to

- Develop and implement a comprehensive AML and KYC policy and Customer Due Diligence Procedures.
- Frequently design and implement suitable training programs for relevant employees including the Board of Directors, in order to effectively implement the regulatory requirements and internal policies and procedures relating to money laundering and terrorist financing risk management.
- Shall develop requirements relating to CDD and ensure that methods are in place to identify any unusual transaction/s and/or transaction pattern which need to be vigilant of and eligible to be reported as suspicious transactions
- Ensuring that all departments of the Company are complying with the policy by way of conducting monitoring, testing and reviews
- Ensure a Compliance report is submitted to the Board of Directors at least annually and to the Risk Committee at appropriate intervals
- Undertaking internal reviews of all suspicions and determining whether or not such suspicions have substance and require disclosure to the FIU at CBSL.
- Obtaining and making use of national and international findings concerning Countries with serious AML deficiencies/Sanctions and informing relevant parties of the Company.
- Adopt the Three line of Defense Framework and carry out the Compliance responsibilities applicable to the second line of defense
- Roll out the Risk based approach for Customer Due Diligence (CDD) and KYC procedures and Implement Risk Profiling of customers of the company
- Ensure that AML related mandatory reporting to the FIU is Carried out in accordance with applicable Laws and Regulations

4.4 Branch Managers/ Business Unit Heads/Department Heads

- Branch Managers/BU heads are responsible for day to day Compliance with Anti Money Laundering obligations within all segments of the Company.
- Ensuring that the Compliance Officer is provided with prompt notification of unusual suspicious transactions and other matters of significance relating to Money Laundering and/or Terrorist Financing.
- Ensuring that all staff members are aware of their obligations and the Company's procedures, and that staff are adequately trained in the area of Anti Money Laundering
- Ensure that all AML breaches including KYC and CDD matters are brought to the notice of the Compliance officer.

4.5 Staff Members

- Remaining vigilant to the possibility of ML/TF.
- Complying fully with all AML/CTF Policies and procedures in respect of customer identification, account monitoring, record keeping and reporting, Risk Profiling and CDD
- Reporting all suspicions of Money Laundering and Terrorist Financing to the Compliance Officer
- All staff are required to read, understand and then accept the AML/CFT policy on an annual basis. Compliance Department along with the Human Resources Department follows up to ensure that all staff comply to this requirement.
- Employees are aware that those who violate any of the regulations or the policies /procedures outlined on AML/CTF, will be subject to disciplinary action on per the Human Resource Policy Frame Work of the Company.
- All staff are mandatorily required to complete both the e learning module and the respective evaluation on an annual basis. The Compliance Department together with the HR Division follows up to ensure that all staff comply to this requirement
- All staff of the company are required to read and understand the Compliance Policy /Manual

Compliance is Everyone's Responsibility

5. LEGAL FRAMEWORK FOR ANTI MONEY LAUNDERING (AML) / COMBATING OF FINANCING OF TERRORISM (CFT) IN SRI LANKA

- For several years government authorities, the Central Bank, the Financial Sector Authorities and Legal and Law Enforcement Authorities, have worked together with international experts to formulate the necessary AML/CFT legal framework for Sri Lanka.
- The Central Bank played a major role in these deliberations not only because it is the institution at the helm of the financial sector, but also because one of its core objectives is the preservation of financial system stability which could be threatened by ML& TF activities.
- The first piece of legislation, the Convention on the Suppression of Terrorist Financing Act, No .25 of 2005 became law on 8th August2005. The other two laws, the Prevention of Money Laundering Act No.5 of 2006 and the Financial Transactions Reporting Act No.6 of 2006 became law on 6th March 2006. All three Acts were prepared in line with the Recommendations provided in the Financial Action Task Force (FATF), and therefore Sri Lanka is compliant with the requirements of the FATF. Convention on the Suppression of Terrorist Financing Act, No.25 of 2005 was amended in 2011 by Convention on the Suppression of Terrorist Financing (Amendment) Act, No.41 of 2011 and Convention on the Suppression of Terrorist Financing (Amendment) Act, No.03 of 2013 while Prevention of Money Laundering Act No.5 of 2006was amended by Prevention of Money Laundering (Amendment)ActNo.40of 2011.Some of the main features of these three Acts are given below.

A) PREVENTION OF MONEY LAUNDERING ACT (PMLA) No. 05 of 2005

- The offence of Money Laundering is defined as receiving, possessing, concealing, investing, depositing or bringing into Sri Lanka, transferring out of Sri Lanka or engaging in any other manner in any transaction, in relation to any property derived or realized directly or indirectly from "Unlawful Activity" or proceeds of "Unlawful Activity".

- Any movable or immovable property acquired by a person which cannot be part of the known income or receipts of a person or money/ property to which his known income and receipts have been converted, is deemed to have been derived directly or indirectly from unlawful activity, in terms of the PMLA.

- PMLA has provisions for a police officer not below the rank of Assistant Superintendent of Police to issue an order prohibiting any transaction in relation to any account, property or investment which may have been used or which may be used in connection with the offence of Money Laundering for a specific period which may be extended by the High Court, if necessary, in order to prevent further acts being committed in relation to the offence.

- Under PMLA following may commit the offence of Money Laundering

a) Persons who commit or have been concerned in the commission of predicate offences, and thereby come into possession or control of property derived directly or indirectly from the commission of such predicate offences

b) Persons who receive possess or come into control of property derived directly or indirectly from the commission of predicate offences, knowing or having reason to believe the true nature of such property (to this group belong persons employed at Financial Institutions) which are used by criminals to launder ill gotten money

- Following are considered as Predicate Offences

Offences under-

- The Poisons, Opium and dangerous Drugs Ordinance
- Laws or Regulations relating to prevention and suppression of terrorism
- The Bribery Act
- Firearms Ordinance,
- Explosives Ordinance, Offensive Weapons Act etc.
- Laws relating to cyber crimes
- Laws relating to offences against children
- Laws relating to offences against trafficking of persons
- Any law punishable with death or imprisonment of seven years or more, whether committed within or outside Sri Lanka

B) FINANCIAL TRANSACTIONS REPORTING ACT NO.6 OF 2006 (FTRA)

- FTRA provides for the setting up of a Financial Intelligence Unit (FIU) as a national central agency to receive analyses and disseminate information relating to Money Laundering and Financing of Terrorism.

- The FTRA obliges institutions, to report to the FIU Cash Transactions and Electronic Fund Transfers above a value prescribed by an Order published in the Gazette. The term "Institutions" covers a wide array of persons and entities. Currently this amount is Rupees One Million (Rs. 1,000,000/-) or its equivalent.

- All suspicious transactions have to be reported by institutions to the FIU irrespective of their magnitude.

- FTRA requires an institution covered by the Act to appoint a Senior Officer as the Compliance Officer who would be responsible for the institution's compliance with the Act.
- The FTRA also requires Supervisory Authorities of Institutions and Auditors to make a Suspicious Transaction Report if they have information which gives them reasonable grounds to suspect that a transaction is related to money laundering or financing of terrorism

- Supervisory Authorities are required by the FTRA to examine whether institutions supervised by them comply with the provisions of the FTRA and to report instances of non compliance to the FIU. Further, they are also required to co-operate with law enforcement agencies and the FIU in any investigation, prosecution or proceeding relating to any act constituting an unlawful activity.

- In terms of the FTRA, institutions are required to engage in Customer Due Diligence (verifying the true identity of customers) with whom they undertake transactions and on going Customer Due Diligence with customers with whom they have a business relationship.

- **The opening and operating of numbered accounts and accounts under a fictitious name are an offence under the FTRA.**

- FTRA makes "tipping-off" an offence (e.g. pre-warning a suspect of an impending investigation).
- In terms of the FTRA, persons making reports under the Act are protected from civil or criminal liability.

- The FIU with Ministerial approval, may exchange information with other FIUs or Supervisory Authorities of a Foreign State.

C.) CONVENTION ON THE SUPPRESSION OF TERRORIST FINANCING ACT NO. 25 OF 2005 AS AMENDED BY ACT NO. 41 OF 2011

- On 10th January 2000, Sri Lanka became a signatory to the International Convention for the Suppression of Terrorist Financing adopted by the United Nations General Assembly on 10/01/2000 and ratified the same on 8/9/2000. The Convention on the Suppression of Terrorist Financing Act. No.25 of 2005 was enacted to give effect to Sri Lanka's obligations under this Convention and further amended under Act No. 41 0f 2011 and Act No. 3 of 2013.

- Under the Act, the provision or collection of funds for use in terrorist activity with the knowledge or belief that such funds could be used for financing a terrorist activity is an offence.
- The penalty for an offence under the Act is a term of imprisonment between 15-20 years and/ or a fine.

- On the conviction of a person for an offence under the Act, all funds collected in contravention of the Act are forfeited to the State.
- The extradition law applies to the offence of financing of terrorism.

30. FINANCIAL INTELLIGENCE UNIT RULE NO.1 OF 2016 – FINANCIAL INSTITUTIONS (CUSTOMER DUE DILIGENCE) RULES

Introduction

Public confidence in financial institutions, and hence their stability, is enhanced by sound financing practices that reduce financial risks to their operations. Money laundering and terrorist financing can harm the soundness of a country's financial system, as well as the stability of individual financial institutions, in multiple ways. Customer identification and due diligence procedures also known as "Know Your Customer" (KYC) rules, are part of an effective Anti Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) regime.

These rules are not only consistent with, but also enhance, the safe and sound operation of financial institutions. While preparing operational guidelines on customer identification and due diligence procedures, financial institutions are advised to treat the information collected from the customer for the purpose of opening of accounts, as confidential and not divulge any details thereof for cross-selling or for any other purpose, and that the information sought is relevant to the perceived risk, is not intrusive and is in conformity with the rules issued here under. These rules are issued under Section 2of the Financial Transactions Reporting Act No.6 of 2006andany contravention of, or non-compliance with the same will be liable to the penalties under the relevant provisions of the Act.

6.1 Provisions on Money Laundering and Terrorist Financing Risk Management Rules

As required by the above rules the Company shall

✓ Conduct following processes in assessing money laundering and terrorist financing risks:

- Documenting the risk assessments and findings
- Considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied
- Keeping the assessment up to date through a periodic review and
- Having appropriate mechanisms to provide risk assessment information to the supervisory authority.

✓ Have proper risk control and mitigation measures including

- Internal policies, controls and procedures to manage and mitigate money laundering and terrorist financing risks that have been identified.
- Management Information systems that provide reliable data on the quantity and nature of Money Laundering/ Terrorist Financing risks and effectiveness with which risks are being mitigated.
- Monitor the implementation of those policies, controls, procedures and enhance them if necessary and
- Take appropriate measures to manage and mitigate the risks, based on the risk-based approach.

✓ **Conduct risk profiling on the customers considering**

- Risk level according to customer category (resident or non- resident, occasional or one off, legal persons, politically exposed persons and customers engaged in different types of occupations)
- Geographical location of business or country of origin of the customer
- Products, services, transactions or delivery channels of the customer (cash based, face to face or non-face to face, cross- border) and
- Any other information regarding the customer

31.THE RISK BASED APPROACH

Risk can be defined as a "Combination of the likelihood of an adverse event occurring and of the potential importance of the damage caused". The Risk Based Approach is a quantitative methodology that will enable the assessment of risks with the aim of mitigating the impact which requires identification of risk factors and classification. The Product Development Committee & the Product Development Department should assess the inherent risks of all products and services existing and that are to be launched in terms of customers, delivery channels, and geographies etc., and evaluate the residual risk based on the available control procedures that are in place to mitigate such risks as per guidelines issued herein

INITIAL ACCEPTANCE

Upon the initial acceptance of a customer, the staff is mandated hereby to ensure that the risk profiling is done by analyzing the Customer profile / nature of business prior to opening of any account in the operating system

Thereafter a regular review and update of the Customer's risk profile based on the level of money laundering and terrorist financing risk the c o m p an y is exposed to. The customers identification records and risk profiles must be updated by the Branch Managers on the following basis.

- High Risk Customers – at least Once a year/ Upon a trigger event
- Medium Risk Customers – Every Three Year / Upon a trigger event
- Low Risk Customers – Every Five Year / Upon a trigger event

Trigger Event

In assessing the materiality and risk of an existing customer, the we should consider the following as a Trigger Events.

"Trigger Event" includes - but is not limited to the following;

a) The nature and circumstances surrounding a particular transaction including the significance of the transaction;
b) Material change in the way the account or business relationship is operated;
c) Any insufficiency of information held on the customer or change in customer's information.
d) Activation of a dormant account/ Sudden activation or change in the manner the account is operating
e) The Customers behavior or sudden change of pattern of the account handling.

8. CUSTOMER DUE DILIGENCE – OVERVIEW

8.1 What is Customer Due Diligence?

All Financial institutions are required to implement a Customer Due Diligence programme (CDD). The regulatory expected outcomes of a Customer Due Diligence program is each company, including LCB Finance PLC should be satisfied that its customers are who they say they are, understand whether its customers are acting on behalf of others and the identity of any beneficial owner(s), and understand its customers' circumstances to guard against the being used for fraud, money laundering or other criminal activity

LCB Finance PLC, along with all other regulated institutions, carry out Due Diligence on their customers to obtain this information and reach this level of comfort. The steps in the Risk Based Due Diligence Process consists of five different aspects.

i.) First Step - Identifying the Customer

The Company needs to obtain the information to establish to their satisfaction the identity of the customer and the intended nature of the business relationship.

There are no exceptions to this requirement. Further details covering this requirement are set out in the company's account opening circular. It shall be the primary responsibility of the employee opening the account to conduct KYC/CDD, and obtain and verify the authenticity of the identification documentation in terms thereof.

ii.) Second Step - Verifying the Customer's Identity

In some cases, the information must then be verified. Information on the customer is obtained directly from the customer and at times from other external sources. Irrespective of how or where the identification information is obtained, a determination must be made whether the information needs to be verified. Verification for this purpose means the information is verified from reliable, independent third-party source(s), and original document being sighted and copies retained been certified as such

iii.) Third Step - Customer KYC Information

In most cases it will be appropriate to know more about the customer than just the identity. For example, there is usually the need to be aware of the nature and scale of business the customer is engaged in and the and surrounding circumstances in addition to the source of funds and/or wealth. This will allow the company to assess the extent to which the customer's transactions and activity with LCB Finance PLC are consistent with the customer's legitimate business. For these purposes, this additional information will be the customer KYC information.

The extent of KYC information to be obtained by the company will depend on the ML/TF Risk Assessment performed by the Entity to ascertain the level of ML risk posed by the customer. In addition to the Local regulators, all major international organizations set out the need to obtain sufficient KYC information, adopting a Risk based focused framework for CDD and to give the appropriate weightage to each risk factor it deems necessary.

iv.) Fourth Step - Obtaining information on the purpose and intended nature of the business relationship

It is important to get information on the purpose and intended nature of the business relationship so as to be able to establish what business the customer is involved in and be able to create a risk profile of the customer. This is essential in order to be able to identify any suspicious activities that seem to be unrelated or not in line with the customer's legitimate business.

v.) Fifth Step - Conducting ongoing monitoring of the business relationship

Ongoing monitoring on customers and their transactions is required by the Regulator and is important in order to detect any suspicious activity not only at the inception of a business relationship or at the occurrence of an occasional transaction but also at later stages throughout the duration of the Business relationship

8.2 Responsibility for Conducting Customer Due Diligence

Responsibility within LCB Finance PLC for conducting the Customer Due Diligence rests with the respective Branch Manager /Counter staff and other staff members within the company as, he who opens the account and manages the relationship retains primary responsibility for the customer relationship

9. ALTERNATIVE REMITTANCE SYSTEMS (HUNDI, HAWALA ETC.)

Extra vigilance is required by the Company to distinguish between formal money transmission services and other money or value transfer systems through which funds or value are moved from one geographic location to another through informal and unsupervised networks or mechanisms. This is required in order to ascertain the sources of such funds and the legitimacy of the transaction/s.

10. DEVELOPING NEW PRODUCTS / USING NEW TECHNOLOGIES

The Management and the Product Development Committee should identify and assess Money Laundering and Terrorist Financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre- existing products. Product development Committee must ensure that Head of Compliance sign off is obtained to proceed and

- ➢ Undertake the risk assessments prior to the launch or use of new products, practices and technologies

- ➢ Take appropriate measures to manage and mitigate the risks which may arise in relation to the development of new products and new business practices

11. OCCASIONAL CUSTOMERS, ONE OFF CUSTOMERS, WALK IN CUSTOMERS AND THIRD PARTY CUSTOMERS

➢ **The Entity shall,**

a. With regard to transactions or series of linked transactions exceeding Rs.200,000/- or its equivalent in any foreign currency conducted by **occasional customers, one off customers or walking customers** conduct CDD measures and obtain copies of identification documents;

b. With regard to **occasional customers, one off customers or walk in customers** who wish to purchase remittance instruments such as **pay orders, drafts exceeding** Rs.200,000/- or its equivalent in any foreign currency conduct CDD measures and obtain copies of identification documents;

c. With regard to all cash deposits exceeding Rs.200,000/- or its equivalent in any foreign currency made into an account separately or in aggregate by a **third-party customer**, have on record the name, address, identification number of a valid identification document, purpose and the signature of the third-party customer.

Under this rule, clerks, accountants, employees, agents or authorized persons of business places who are authorized to deal with the accounts shall not be considered as a third party.

Also, if the Company has reasonable grounds to suspect that the transaction or series of linked transactions are suspicious or unusual, the Company shall, obtain such information irrespective of the amount specified above.

12. CDD FOR LEGAL PERSONS AND LEGAL ARRANGEMENTS

➢ **The Company shall in the case of a customer that is a legal person or legal arrangement,**

a. Understand the nature of the business of the customer, its ownership and control structure;
b. Identify and verify the customer in terms of the requirements set out below.

➢ **In order to identify the natural person if any, who ultimately has control ownership interest in a legal person, the Company shall at the minimum obtain and take reasonable measures to verify the following**

a. Identity of all Directors and Shareholders with equity interest of more than 10% with the requirement imposed on the legal person to inform of any change in such Directors and Shareholders;

b. If there is a doubt as to whether the person with the controlling ownership, interest is the beneficial owner or where no natural person exerts control through owner ship interest, the identity of the natural person, if any, exercising control of the legal person or arrangement through independent sources;

c. Authorization given for any person to represent the legal person or legal arrangement either by means of Board Resolution or otherwise;

d. Where no natural person is identified under the preceding provisions, the identity of the relevant natural persons who hold the positions of senior management;

e. When a legal person's controlling interest is vested with another legal person, the Company shall identify the natural person who controls the legal person.

➢ **In order to identify the beneficial owners of a legal arrangement, the Company shall obtain and take reasonable measures to verify the following**

a. For Trusts, the identities of the author of the Trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the Trust (including those who control through the chain of control or ownership); or

b. For other types of legal arrangements, the identities of persons in equivalent or similar positions.

13. NON-GOVERNMENTAL ORGANIZATIONS, NOT FOR PROFIT ORGANIZATIONS OR CHARITIES

➢ **The Company shall conduct enhanced CDD measures when entering in to a relationship with a Non Governmental Organization (NGO) or a Non Profit Organization (NPO) and Charities to ensure that their accounts are used for legitimate purposes and the transactions are commensurate with the declared objectives and purposes.**

1. The Company shall open accounts in the name of the relevant NGO, NPO or Charity as per title given in the constituent document thereof.
2. The individuals who are authorized to operate the account and members of their governing bodies shall also be subject to enhanced CDD measures.
3. The Company shall ensure that the persons stated in(2) above are not affiliated with any entity or person designated as a prescribed entity or person, whether under the same name or a different name.

➢ **The Company shall not allow personal accounts of the members of the governing bodies of a NGO, NPO or Charity to be used for charity purposes or collection of donations.**

1. The Company shall review and monitor all existing relationships of a NGO, NPO or Charity to ensure that those organizations, their authorized signatories, members of their governing bodies and the beneficial owners are not linked with any entity or person designated as a prescribed entity or person, either under the same name or a different name.
2. In case of any suspicion on similarity in names, the Company shall file a Suspicious Transaction Report or take other legal action or take both steps.

14. CUSTOMERS AND FINANCIAL INSTITUTIONS FROM HIGH-RISK COUNTRIES

- The Company shall apply the enhanced CDD measures to business relationships and transactions to customers and Financial Institutions from high-risk countries.
- The Secretary to the Ministry of the Minister to whom the subject of Foreign Affairs has been assigned or the subject of Defence has been assigned, as the case may be, shall specify the high-risk countries referred above.

1. based on the Financial Action Task Force listing; or
2. independently taking into account, the existence of strategic deficiencies in anti money laundering and combating of financing of terrorism policies and not making sufficient progress in addressing those deficiencies in those countries.
3. Upon specifying the high-risk countries as specified in (2) above the Company shall publish the list of high-risk countries in its official website.
4. The type of enhanced measures applied under (1) above shall be effective and correspond to the nature of risk.

- In addition to enhanced CDD measures, the Company shall apply appropriate counter measures, as follows, for countries specified in the list of high-risk countries referred to in (2) above, corresponding to the nature of risk of listed high-risk countries

a. Limiting business relationships or financial transactions with identified countries or persons located in the country concerned;

b. Review and amend or, if necessary, terminate, correspondent banking relationships with Financial Institutions in the country concerned;

c. Conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the Financial Institution or financial group, located in the country concerned; and d. Conduct any other measures as may be specified by the Financial Intelligence Unit

15. POLITICALLY EXPOSED PERSONS (PEPS)

Guideline No.3 of 2019 issued by Financial Intelligence Unit of Central Bank of Sri Lanka which shall be read together with the Financial Transactions Reporting Act No 6 of 2006 and Financial Institutions (Customer Due Diligence) Rules No 1 of 2016 provides the Companies with a set of instructions on the definition, identification, reviewing and managing the risk associated with PEPs. Accordingly, the Company has taken steps to identify and mitigate the risk associated with PEPs.

➢ In relation to politically exposed persons or their family members and close associates, the Company shall-

a. Implement appropriate internal policies, procedures and controls to determine if the customer or the beneficial owner is a politically exposed person;

b. Obtain approval, before or after entering into the relationship from the Senior Management of the Company to enter into or continue business relationships where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

c. Identify, by appropriate means, the sources of funds and wealth or beneficial owner ship of funds and wealth; and

d. Conduct enhanced ongoing monitoring of business relationships with the politically exposed person.

➢ The Company is aware that business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves and also that the definition is not intended to cover middle ranking or more junior officials in the foregoing categories. (**More Details - refers to PEPS Policy**)

16. WIRE TRANSFERS

- The Company shall in processing wire transfers, take freezing action and comply with prohibitions on conducting transactions with designated persons or entities, and any other person and entity who acts on behalf of or under the direction of such designated persons or entities or for the benefit of such designated persons or entities, in terms of any regulation made under United Nations Act No.45 of 1968, giving effect to United Nations Security Council Resolutions on targeted financial sanctions related to terrorism and terrorist financing and proliferation of weapons of mass destruction and its financing or in terms of any other regulation made under the said Act giving effect to any other United Nations Security Council Resolution.

- The Company shall preserve Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages that accompany inward remittances for a period of 12 years from the date of transaction.

- The Company shall ensure that all cross-border wire transfers to be always accompanied with the following: -

(a) Originator information: -

(i) name of the originator;

(ii) originating account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

(iii) originator's address, national identity card number or any other customer identification number as applicable;

(b) beneficiary information: -

(i) name of the beneficiary; and

(ii) beneficiary account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

- Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country and shall include the originator's account number or unique transaction reference number.

- The Company shall verify the information pertaining to its customer where there is a suspicion of money laundering and terrorist financing risk.

- In the case of domestic wire transfers, the Company shall ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers unless such information can be made available to the Beneficiary Financial Institution and appropriate authorities by other means.

- ➢ In the case where the information accompanying the domestic wire transfer can be made available to the Beneficiary Financial Institution and appropriate authorities by other means, the Company shall include the account number or a unique transaction reference number, provided that any such number will permit the transaction to be traced back to the originator or the beneficiary.
- ➢ The Company shall maintain all originator and beneficiary information collected, in accordance with the Act.
- ➢ At instances where the requirements specified above could not be complied with, the Company shall not proceed with the wire transfer unless directed to do so by the Financial Intelligence Unit and shall consider reporting the relevant transaction as a suspicious transaction to the Financial Intelligence Unit.

17. ACCOUNT OPENING GUIDANCE

Face to Face (Check list – attachment I)

1. Individual Customer

(a) The following information shall be obtained:

In the case of all customers

- Full name as appearing in the identification document;
- Official personal identification or any other identification document that bears a photograph and the NIC Number of the customer (ex: National Identity Card for citizens of Sri Lanka and valid Passport for foreigners)
- Permanent address as appearing on the identification document. If residential address differs from the permanent address residential address shall be supported by a utility bill not over three months old or any other reliable proof of residence. Utility bills are to be specified as electricity bill, water bill and fixed line telephone operator's bill. No post box number shall be accepted except for state owned enterprises. In the case of "C/O", property owner's consent and other relevant address verification documents are required to be obtained.
- Telephone number, fax number, and e-mail address;
- Date of birth;
- Nationality;
- Occupation, business, public position held and the name of employer and geographical areas involved;
- Purpose of which the account is opened;
- Expected turnover/ volume of business;
- Expected mode of transactions;
- Satisfactory reference as applicable; and

In the case of non- resident customers

- The reason for opening the account in Sri Lanka
- Name, address and the copy of passport of the person or persons authorized to give instrictions

The following documents shall be obtained (each copy shall be verified against the original)

- Copy of identification document;
- Copy of address verification document;
- Copy of the valid visa/permit in the case of accounts for non national customers.

2. Proprietorship/ Partnership Accounts

(a) The following information shall be obtained

- Full names of the partners or proprietors as appearing in the business registration document; Nature of the business;
- Registered address or the principal place of business;
- Identification details of the proprietor/ partners as in the case of individual accounts;
- Contact telephone or fax number;
- Income Tax file number;
- The extent of the ownership controls;
- Other connected business interests

(b) The following documents shall be obtained (each copy shall be verified against the original)

- Copy of the business registration document
- Proprietors' information/ Partnership Deed;
- Copy of identification and address verification documents.

3. Corporation/ Limited Liability Company

(a) The following information shall be obtained

- Registered name and the Business Registration Number of the institution;
- Nature and purpose of business;
- Registered address of principal place of business;
- Mailing address, if any;
- Telephone/ Fax/ email;
- Income Tax file number;
- Bank references (if applicable)
- Identification of all Directors as in the case of individual customers;
- List of major shareholders with equity interest of more than ten percent;
- List of subsidiaries and affiliates;
- Details and the names of the signatories.

In the case of companies listed on the Stock Exchange of Sri Lanka licensed under the Securities and Exchange commission of Sri Lanka Act No. 36 of 1987 or any other stock exchange subject to disclosure requirements ensuring adequate transparency of the beneficial ownership, the Bank may use the information available from reliable sources to identify the Directors and major shareholders.

(b) The following documents shall be obtained (each copy shall be verified against the original)

- Copy of the Certificate of Incorporation;
- Copy of Form 40 (Registration of an existing company) or Form 1 (Registration of a company) under the Companies Act and Articles of Association;
- Board Resolution authorizing the opening of the account;
- Copy of form 20 (change of Directors/ Secretary and particulars of Directors/ Secretary) under the Companies Act;
- Copy of form 44 (full address of the registered or principal office of a company incorporated outside Sri Lanka and its principal place of business established in Sri Lanka) under the Companies Act;
- Copy of Form 45 List and particulars of directors of a company incorporated outside Sri Lanka with a place of business established in Sri Lanka) under the Companies Act;
- Copy of the Board of Investment Agreement, if a Board of Investment approved company;

- Copy of the export Development Board (EDB) approved letter, if EDB approved company;
- Copy of the certificate to commence business, if a public quoted company;
- Name of the person or persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board resolution as the case may be;
- Latest audited accounts if available.

The above documents shall apply to a company registered abroad as well. The non documentary method in the absence of the above documents would entail a search at the Credit Information Bureau (CRIB), bank references, site visits and visiting the business website of the customer.

4. Clubs, Societies, Charities, Associations and Non Governmental Organization

(a) The following information shall be obtained

- Registered name and the registration number of the institution;
- Registered address as appearing in the Charter, Constitution etc.;
- Identification of at least two office bearers, signatories, administrators members of the governing body or committee or any other person who has control and influence over the operations of the entity as in the case of individual accounts;
- Committee or Board Resolution authorizing the account opening;
- The source and level of income funding;
- Other connected institutions/ associates/ organizations;
- Telephone/ facsimile number/ email address

(b) The following documents shall be obtained and be verified against the original

- Copy of the registration document/ Constitution/ Charter etc.;
- Board Resolution authorizing the account opening;
- Names of the persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board/ Committee Resolution.

➢ Bank accounts for charitable and aid organizations and Non Government Organizations (NGO)s should be opened only with the registration of the regulatory authority empowered to regulate charitable and aid organizations, non-governmental organizations and non-profit organizations for the time being and with other appropriate credentials. Due regard should be paid to specific directions governing their operations i.e. issued by the Department of Bank Supervision and Department of Supervision of Non Bank Financial Institutions of the Central Bank and the Director- Department of Foreign Exchange.

5. Trusts Nominees and Fiduciary Accounts

(a) The following information shall be obtained

- Identification of all trustees, settlers, grantors and beneficiaries in case of trust as in the case of individual accounts;
- Whether the customer is acting as a 'front' or acting as a trustee, nominee or other intermediary.

(b) The following documents shall be obtained and be verified against the original

- Copy of the Trust Deed as applicable;
- Particulars of all individuals.

6. Stocks and Securities Sector specific requirements

(a) The following information shall be obtained from the Funds approved by the Securities and Exchange Commission of Sri Lanka

- Name of the Fund;
- Purpose of the fund;
- Place of establishment of the Fund;
- Details (name, address, description etc.) of the Trustee/ Manger of the Fund;
- If the Trustee/ manger is a company, date of incorporation, place of incorporation, registered address of such trustee/ Manager;
- Copies of the document relating to the establishment and management of the fund; (ex: prospectus, Trust Deed, Management Agreement, Bankers Agreement, Auditors Agreement);
- Copy of the letter of approval of the fund issued by the supervisory authority of the relevant country;
- Copy/ copies of the relevant Custody/ Agreement;
- Details of beneficiaries.

(b) Certification requirement-

All supporting documents to be submitted to Central Depository System shall be certified, attested or authenticated by the person specified in (A) or (B) below for the purpose of validating the applicant-

(A) For non-resident applicant-

- By the Company Registrar or similar authority;
- By a Sri Lankan Diplomatic Officer or Sri Lankan Consular Officer in the country where the documents were originally issued;
- By a Solicitor, an Attorney-at-Law, a Notary Public practicing in the country where the applicant resides;
- By the Custodian Bank;
- By the Global Custodian (the Custodian Bank shall certify the authenticity of the signature of the Global Guardian) or
- By a Broker.

(B) For resident applicants-

- By the Registrar of Companies or the Company Secretary (applicable in respect of corporate bodies);
- By an Attorney-at- Law or a Notary Public;
- By a Broker; or
- By the Custodian Bank.

The person certifying shall place the signature, full name, address, contact telephone number and the official seal (Not applicable for Brokers, Custodian Banks and Global Custodians)

Where the application is titled in the name of the 'Registered Holder/ Global Custodian/ Beneficiary' and forwarded through a Custodian Bank, a copy of the SWIFT message or similar document issued by the Global Custodian instructing the local Custodian bank to open the account on behalf of the Beneficiary company shall be submitted together with a Declaration from the Global Custodian that a custody arrangement or agreement exist between the Global Custodian and Beneficiary.

18. GENERAL PROVISIONS

1. The Company is required to appoint a Key Management Person who is from Senior Management level of the Company as the Compliance Officer, who shall be responsible for ensuring the institution's compliance with the requirements of the Act and the above said Rules.

2. Ensure that the Compliance Officer or any other persona authorized to assists him or act on behalf of him has prompt access to all customer records and other relevant information which may be required to discharge their functions.

3. Develop and implement a comprehensive employee due diligence and screening procedure to be carried out at the time of appointing or hiring of all employees whether permanent, contractual or outsourced.

4. Frequently design and implement suitable training programmes for relevant employees in order to effectively implement the regulatory requirements and internal policies and procedures relating to money laundering and terrorist financing risk management.

5. Maintain an independent audit function incompliance with the Code of Corporate Governance issued by the Central Bank of Sri Lanka that is adequately resourced and able to regularly assess the effectiveness of the internal policies procedures and controls of the Company and its compliance with regulatory requirements.

6. Implement group wide programmes which shall be applicable and appropriate for all branches and majority owned subsidiaries with a view of combating money laundering and terrorist financing activities and shall include following in addition to the rules set above.

- ✓ Initiate measures and procedures for sharing information required for the purpose of conducting CDD and money laundering and terrorist financing risk management;
- ✓ Provide information of customers, accounts and transactions and of audits, with group level compliance from all branches and subsidiaries of the financial group when necessary for implementing the suppression of money laundering terrorist financing measures and
- ✓ Maintain adequate safeguards on the confidentiality and use of information exchanged among the branches and subsidiaries of the financial group.

19. APPLICABILITY OF FIU RULE NO. 01 OF 2016

This section of the Policy is to ensure that LCB Finance PLC has internally developed effective Anti Money Laundering and Combating of Financing of Terrorism procedures to reduce the risk of the Company being used in money laundering transactions, in addition to the requirements of the legislation and the FIU Rule No. 1 of 2016 as set out in Chapter 3.

It is the Policy of the Company to prevent the use of its facilities for the laundering of money derived from Criminal activities. All Employees must be alert to the possibility of the Company being unwittingly involved in the activities of third parties, who may seek to use Company facilities to hide the source of criminal funds.

As such,

- ✓ The Company has formulated this Policy which is approved by the Board of Directors prepared subject to the written laws in force for the time being, on anti-money laundering and suppression of terrorist financing
- ✓ The area of coverage of this Policy among other things, include risk assessment procedures, CDD measures, manner of record retention, handling wire transfers, the detection and internal reporting procedure of unusual and suspicious transactions and the obligation to report suspicious transactions to the Financial Intelligence Unit
- ✓ Detailed procedures and controls have been developed in compliance with this Policy. Circulars are issued from time to time setting out the new standards and requirements of Know your Customer and Customer Due Diligence concept.

Additionally, FIU Rule No. 01 of 2016 also provides for the update of the existing customer records in accordance with the CDD rules and acting in compliance with this rule, Managers/ Department Heads are required to submit a monthly status report of same to the Compliance Department. Compliance Department shall report the status monthly to the Board of Directors

20. CAPTURE THE INFORMATION REQUIRED UNDER THE RULES OF THE FINANCIAL INTELLIGENCE UNIT

In order to comply with the requirements in Direction No. 01 of 2016, it is necessary to obtain KYC Information for all Accounts opened at the branches.

The following are the broad guidelines in this regard:

1. Individual/Joint Accounts

a) The individual Account opening/Mandates and information profile of the customers (KYC Form) which is prepared incorporating the basic requirements should be duly completed by the Customer/s and also signed by them as being correct. An authorized officer must put his signature in this document to certify that the information was provided in his/her presence and the Manager, after perusing all account opening documents must sign the mandate certifying the accuracy of the documents obtained.

b) The Branch Manager should also fill out the Risk Categorization form as a means of assessing the risk of Money Laundering/Terrorist Financing, before the end of each working day for accounts opened on a particular date. This is the responsibility of the Branch Manager.

The branch network is also required to monitor the transactions of

- high risk customers at every transaction,
- medium risk customers as and when necessary and
- low risk customers if a suspicious transaction takes place

c) The Departments/branch network are required to retain and keep in the custody of the Company-

- A photocopy of the identification document

- A copy of the Address Verification Document, in the event, the current address of the customer differs from that of the Identification Document
- Any other additional document specified in Chapter 3.

2. Proprietorship/ Partnership/ Company/ Trust/ NGO/ Charitable Organization/ Club/ Society etc.

a) The Account opening Form/Mandate and the KYC must be obtained for these customers and they should be filled by the Customer and signed by the Delegated Representative of the Customer as being correct.

b) Additionally, for

i) Companies

Each Director should complete an individual profile of the customer (KYC) form in addition to the KYC form for the company.

ii) Proprietor/ Partnership

An individual profile of the customer (KYC) form in addition to the KYC form for the proprietor/partnership.

iii) Trusts

Each Trustee should complete an individual profile of the customer (KYC)form

iv) NGOs/ Charities/ Clubs/ Societies/ Other

02 office bearers who are the authorized signatories of the entity to complete individual profile of the customer (KYC) form

c) Copies of all documents as applicable as set out in this Policy have to be retained by the Company

d) The Branch Manager should also fill out the Risk Categorization form as a means of assessing the risk of Money Laundering/ Terrorist Financing, before the end of each working day for accounts opened on a particular date

20.1 General Guidelines

1. All staff members are required to comply with the FIU Directives on Know Your Customer (KYC) and Customer Due Diligence (CDD) at all times. This has been communicated through the Compliance Officer's Circular Letter No.6552/2007 dated 4th September 2007 and Compliance Officer Circular Letter Nos. 6552/2007(1) dated 24.8.2012 and 6552/2007(2) dated 15.3.2016.
2. It is the responsibility of the Branch Managers and Heads of Department to educate employees coming under their purview of the importance of KYC and CDD and the requirements on Customer Identification. Special emphasis must be made to train the Account Opening Officers in this regard.

3. A Certificate on Compliance with the procedures contained in this Policy; would need to be submitted by the Branch Managers to the Compliance Officer, on a monthly basis.

4. The following important provisions are further highlighted:

i) Satisfactory reference has to be obtained for all Current Accounts. For other accounts, it will be at the discretion of the Branch Manager on a Risk Assessment Basis.

ii) No account should be opened, unless and until proper identification and information pertaining to a prospective client is obtained, except as follows: The following exception procedures are laid down where compliance has not been possible, with the above.

a) It may be acceptable to allow minor accounts to be opened pending completion of KYC requirements on documentation, within 3 months of opening the account.

b) Where such accounts have been opened as in (a) above, they have to be recorded in a Register called the KYC Exception Register and it shall be initialed by the Branch Manager on a daily basis and on Branch inspection visits by the Compliance Officer or Assistant Compliance officer

c) Outstanding KYC documentation should be obtained before the expiry of 3 months from the date of the opening of such account – in order to continue the account.

d) Where such accounts have been opened, funds should not be paid out of the account, until such time as the KYC documentation is completed.

21. SUSPICIOUS TRANSACTION/BUSINESS

As per Section 7 of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA);

"Where an Institution –

(a) has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence; or

(b) has information that it suspects may be relevant –

(i) to an act preparatory to an offence under the provisions of the Convention on the Suppression of Financing of Terrorism Act, No. 25 of 2005;

(ii) to an investigation or prosecution of a person or persons for an act constituting an unlawful activity, or may otherwise be of assistance in the enforcement of the Money Laundering Act, No. 05 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005,

The Institution shall, as soon as practicable, after forming that suspicion or receiving the information, but no later than two working days there from, report the transaction or attempted transaction or the information to the Financial Intelligence Unit"

Also, under section 14(1)(b)(iv) of the Act the Company has to establish and maintain procedures and systems to implement the reporting requirement under Section7 of the FTRA. Further, Section14(1)(d) requires the Company to train its officers employees and agents to recognize suspicious transactions.

Whilst all unusual transactions are not automatically linked to Money Laundering, unusual transactions become suspicious if they are considered inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account.

21.1 Suspicious Cash Transactions

- Unusually large cash deposits made by an individual or a company whose normal business activity would mainly be conducted by cheques or other instruments.
- Substantial increase in cash deposits by any customer or the Company without an apparent cause, especially if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customers.
- Customers who deposit Cash in numerous stages so that the amount of each deposit is small, but the total of which is equal to or exceeds the reporting threshold amount
- Customer accounts whose transactions, both deposits and withdrawals are mainly conducted in cash rather than in negotiable instruments (e.g. cheques, letters of credit, draft etc.) without an apparent reason.

21.2 Suspicious Transactions using Customers' Accounts

- Customers who maintain a number of trustee or customers' accounts which are not required by the type of business they conduct particularly, if there were transactions which contain names of unknown persons.
- Customers who have multiple accounts and pay-in amounts of cash to each of these accounts, whereby the total of credits is a large amount except, for institutions which maintain these accounts for financial relationships with company which extend them facilities from time to time
- Any individual or company whose account shows virtually no normal personal financing or business-related activities, but is used to receive or disburse large sums which have no obvious purpose or for a purpose not related to the account holder and/or his business
- Customers who have accounts with several financial institutions within the same locality and who transfer the balances of those accounts to one account and subsequently transfer the consolidated amount to a person abroad.
- A large number of individuals who deposit monies into the same account without an adequate explanation.

- Unusually large deposits to accounts that have never witnessed such deposits particularly, if a large part of these deposits is in cash.

21.3 DESCRIPTION OF SUSPICIOUS TRANSACTION

(1) Activating of dormant account
(2) Large/Unusual cash deposit/withdrawal not consistent with the known pattern of transactions
(3) Frequent transactions below the mandatory reporting threshold level (Rs. 1,000,000)
(4) Customer suspected of having terrorist links
(5) Funds originating from a suspicious organization/individual (known terrorist front organizations, shell companies etc.)
(6) Reluctance to divulge identification and other information
(7) Transaction without an economic rationale

21.4 SUSPICIOUS LOAN TRANSACTIONS:

- Customers who repay classified/problem loans before the expected time and in larger amounts than anticipated.
- Customers who request loans against assets held by the financial institutions or third party, where the origin of these assets is not known, or the assets are inconsistent with the customer's standing.

22. RISK MITIGATING ON CUSTOMER TRANSACTIONS

It is imperative that company has placed proper controls to mitigate the AML risk to the Company at customer on boarding and transaction processing. In this regard company has placed following controls to identify suspicious transactions and customers with negative records.

i. Transaction Monitoring

Ongoing Monitoring:

The Company and its employees are required to monitor transactions to determine if any particular transaction is suspicious in nature and may be related to money laundering or terrorist financing activities. The extent of the monitoring will be determined on a risk-based approach. Ongoing monitoring is an important part of the Company's anti- money laundering and suppression of terrorist financing program.

Post transaction AML Monitoring

a) Transaction monitoring system (Core System)

Company has established a transaction monitoring system (through core system) to identify/ track suspicious transactions and transaction trends to ascertain whether transactions are consistent

and in line with the customers' known profile. Respective staff members are required to be well acquainted with the system.

System also shall be used to risk rate customers in terms of CDD gazette

b) Manual transactions monitoring based on exceptional reports other than System.

Further manual transactions monitoring process is being carried out by the compliance staff on an exceptional basis, based on the system generated Reports. The transactions monitored may include Cash Deposit, EFT transfers and wire transfers

ii. Sanction Program

The company must verify whether any prospective customer or beneficiary appears on any suspected terrorist list or alert list issued in compliance with the United Nations Regulations No. 1 of 2012 published in Gazette Extraordinary No. 1758/19 dated May 15, 2012 and United Nations Regulations No. 2 of 2012 published in Gazette Extraordinary No. 1760/40 dated May 31, 2012, relating to the prevention and suppression of terrorism and terrorist financing, inclusive of United Nations Security Council Resolutions 1267 and 1373 and any successor resolutions thereto

The Company is keen in managing financial crime risks that are inherent in customer relationships. Thus, the Company takes efforts to gain reassurance that the risks of on-boarding and continuous transactions with customers are managed appropriately in respect of following;

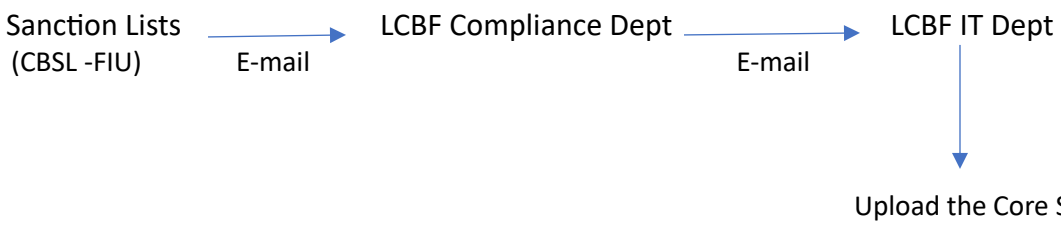
i. Any type of sanction that has been made into Law of the country or as issued as a directive by respective regulatory authority with specific authority to banks or that has an indirect compliance requirement.

ii. Internationally Sanctioned Countries and Designated Persons by the United Nations

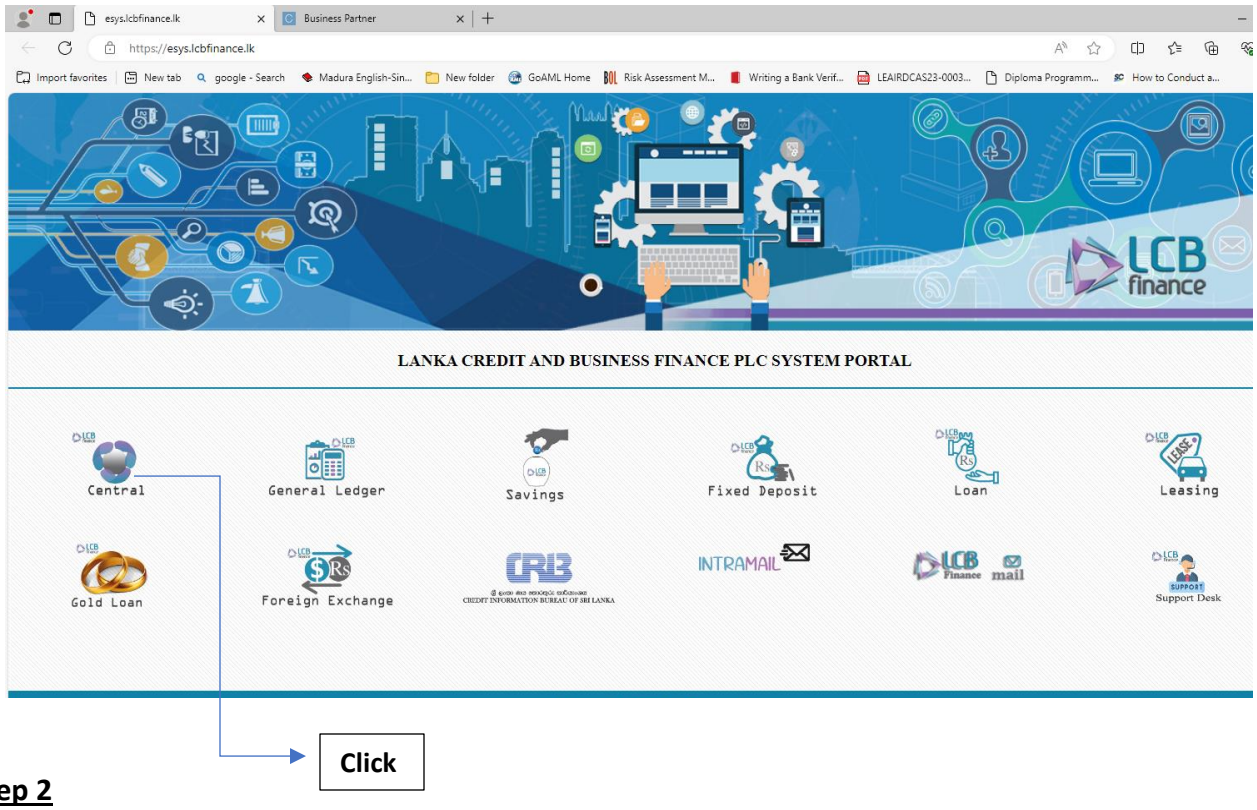
iii. Sanction Programs of Office of Foreign Assets Control (OFAC)

iv. Any other international sanctioned program that would have an impact on Financial Relationships as decided by the Compliance Officer time to time

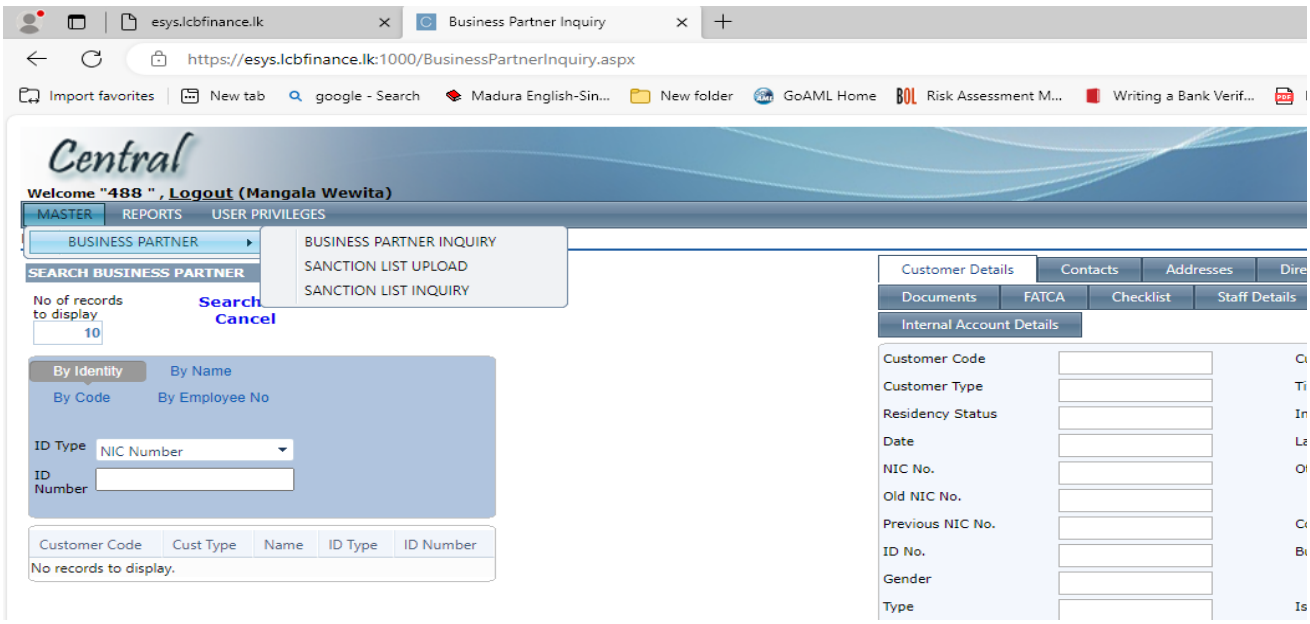
iii. Sanction List update and Screening procedure



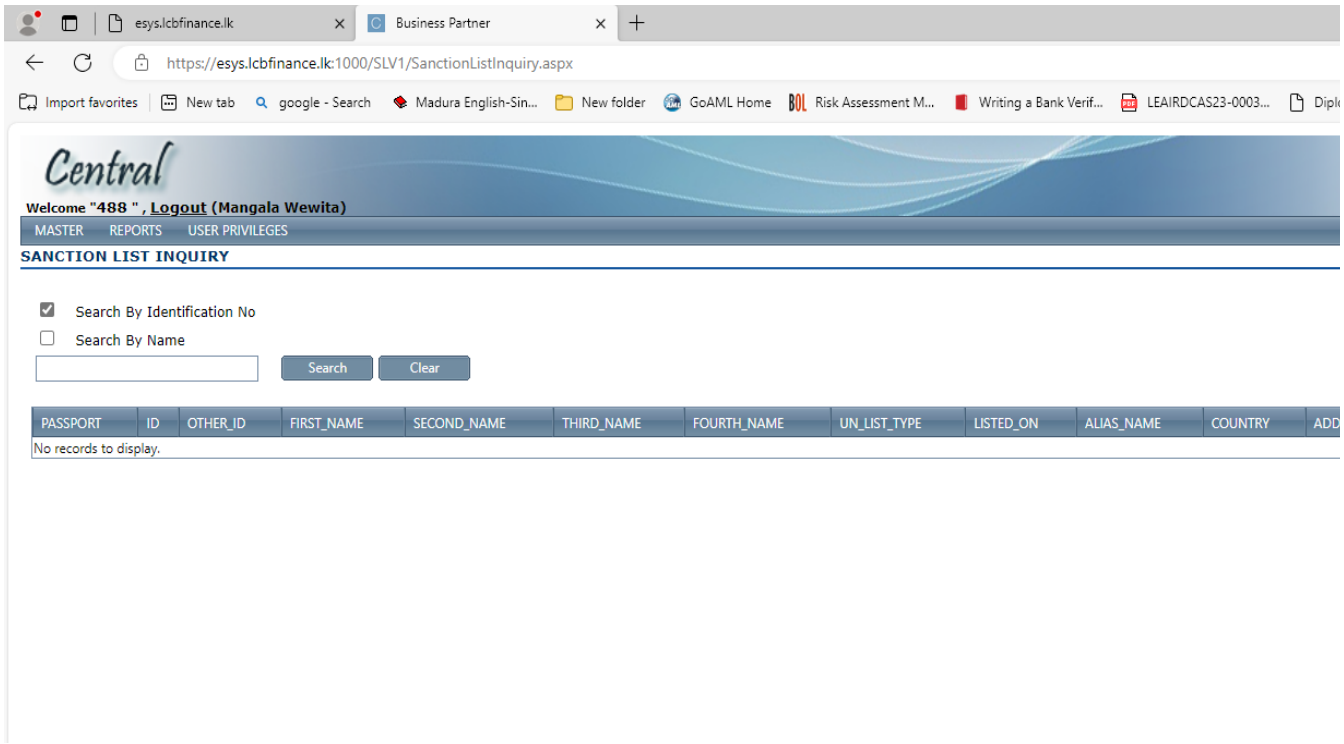
Step 1


esys.lcbfinance.lk
Business Partner
https://esys.lcbfinance.lk
LCB finance
LANKA CREDIT AND BUSINESS FINANCE PLC SYSTEM PORTAL
Central
General Ledger
Savings
Fixed Deposit
Loan
Leasing
Gold Loan
Foreign Exchange
CRIB
INTRAMAIL
LCB Finance mail
Support Desk
Click

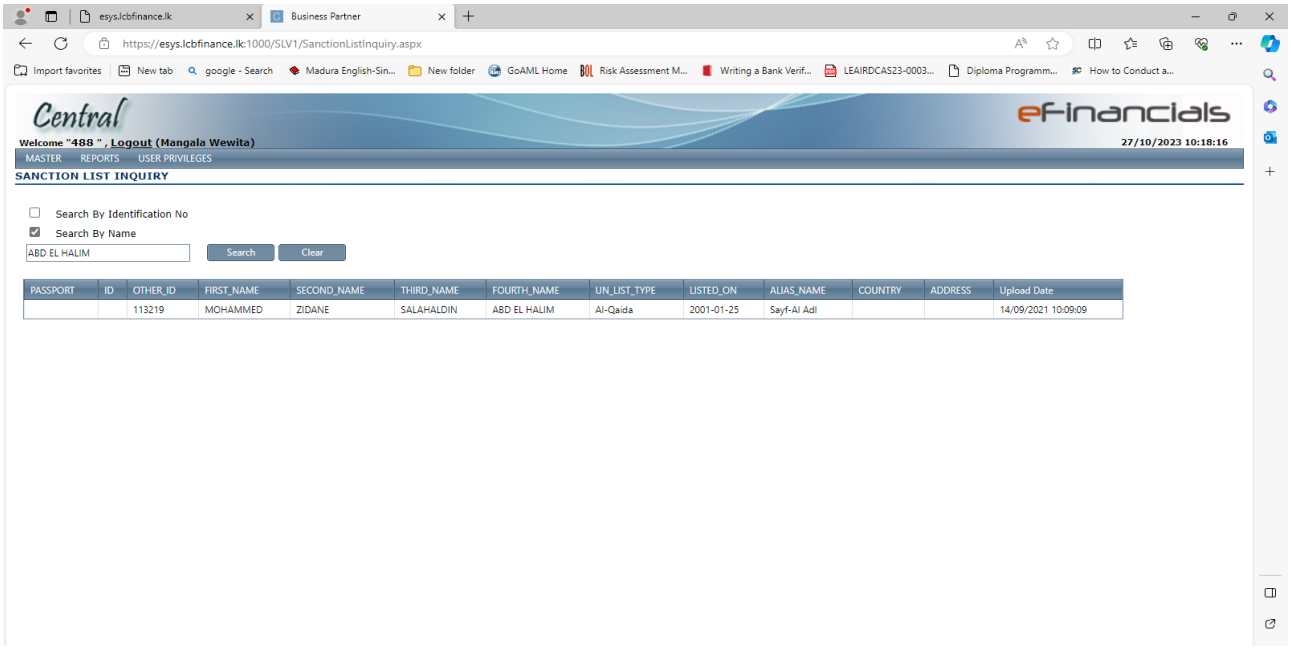
Step 2


esys.lcbfinance.lk
Business Partner Inquiry
https://esys.lcbfinance.lk:1000/BusinessPartnerInquiry.aspx
Central
Welcome "488 " , Logout (Mangala Wewita)
MASTER
REPORTS
USER PRIVILEGES
BUSINESS PARTNER
BUSINESS PARTNER INQUIRY
SANCTION LIST UPLOAD
SANCTION LIST INQUIRY
SEARCH BUSINESS PARTNER
No of records to display
10
Search
Cancel
By Identity
By Name
By Code
By Employee No
ID Type
NIC Number
ID Number
Customer Code
Cust Type
Name
ID Type
ID Number
No records to display.
Customer Details
Contacts
Addresses
Documents
FATCA
Checklist
Staff Details
Internal Account Details
Customer Code
Customer Type
Residency Status
Date
NIC No.
Old NIC No.
Previous NIC No.
ID No.
Gender
Type

Step-3



Step-4



22.1 Reporting requirements for Suspicious Transactions

A suspicious transaction will often be inconsistent with a customer's known legitimate business or employment or personal activities. It will also be inconsistent with normal business of similar accounts.

Suspicious transaction reporting procedure:

i. If a staff member suspects or has reasonable grounds to suspect or has an honest belief that the funds or proceeds of an unlawful activity or related to terrorist financing, it should promptly informed and a suspicious transaction report (STR) should be sent to the Compliance Officer. Suspicious transactions shall be reported to the Compliance Officer or via e-mail or through the Phone.

ii. The Compliance Officer or designate will examine such report and where necessary call for supporting document and if the suspicion still prevails, the Compliance Officer soon as practicable, but not later than two working days, report the transaction or attempted transaction or the information to FIU (through goAML system).

Confidentiality and Non-disclosure

i. Under no circumstances should any staff member of the bank disclose to the customer or any other person or body of persons that a disclosure has been made to the FIU or any information that will identify or is likely to identify the person who handled or reported the suspicious transaction, which will constitute an offence under the FTRA.

ii. No staff member when making a suspicious report should make any false or misleading statement deliberately or make any omission from any statement thereby making it false or misleading.

iii. No staff member should divulge that an investigation into an offence of money laundering is being or is to be conducted.

iv. No staff member should destroy or falsify any documents likely to be relevant to the investigation.

v. All staff is required to co-operate with the investigations relating to money laundering by such authorities or regulations

RECORD RETENTION PERSONAL CRIMINAL LIABILITY

i. As per the anti-money laundering legislation in Sri Lanka, any offence under the Act will give rise to a potential personal criminal liability. Therefore, strong disciplinary action will be taken against any member of staff who fails, without reasonable excuse, to make a report on a suspicious transaction.

ii. Disciplinary action will also be initiated against any member of staff who blocks, or attempts to block, a report by another member of staff. Protection of persons reporting suspicious transactions No Civil, Criminal or disciplinary or reprisal action shall be initiated against any staff member who reports suspicious activity in good faith in terms of the FTRA and in terms of this Policy and the confidentiality of such reporting person shall be protected to assist the authorities when investigating cases of suspected money laundering, it is essential that evidence of customer identification, address verification and all transactions is retained for at **least six years.**

iii. Company shall retain prescribed records of identification, pertaining to information gathered, mandates, and documents relating to transactions for a **minimum of six years.**

iv. Following records /reports shall be retained for a period of at least six years after the relationship with the customer has ended.

- Identification and account opening records
- Documents verifying evidence of identity (including address)
- Non-account holders identifications
- Account transaction records
- Every transaction undertaken for a customer
- Records relating to training internal and external,
- Records of compliance monitoring of transactions
- Suspicious Transaction Reports
- Documentary evidence of any action taken in response to internal and external reports of suspicious transactions
- Mandatory transaction Reports (CTR, EFT – In and Out)

v. Records will be retained in hard copy, on microfiche or computer, or other electronic format and shall be available within a reasonable time to Compliance Officer and to the investigating authorities.

vi. Officers responsible to retain transactions records electronically shall ensure that transactional records are not lost before the six years retention period or expires as a direct consequence of automatic data retention constraints.

vii. Where it is known that an investigation is ongoing, the relevant records will be retained until the authorities inform the company otherwise

23. IDENTIFICATION OF BENEFICIAL OWNERS

The "Beneficial Owner" of the legal person or legal arrangement is a natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted including the person who exercises ultimate effective control over a person or a legal arrangement, wherein the controlling ownership having 10% (ten percent) or more of the capital of a legal person. (FIU Guidelines issued on Identification of Beneficial Owners, No 04 of 2018)

The Company's responsibility to determine the natural person(s) who is/are the Ultimate Beneficial Owner(s).

The UBO must be a natural person and cannot be a company, an organization or a legal arrangement. There may be more than one beneficial owner associated with a customer.

If the customer is a natural person, the person can be treated as the beneficial owner unless there are reasonable grounds to show that he/she acting on behalf of another or if another person is the beneficial owner of the property of the customer.

Requirements for opening of accounts

In order to identify the natural person Ultimate Beneficial Owner (UBO) if any, who ultimately has controlling ownership interest in a legal person, the company at the minimum shall obtain and take reasonable measures to verify the following: -

a. Identity of all Directors and Shareholders with equity interest of more than ten per cent (10%) with the requirement imposed on the legal person to inform of any change in such Directors and Shareholders;
b. If there is a doubt as to whether the person with the controlling ownership, interest is the beneficial owner or where no natural person exerts control through ownership interest, the identity of the natural person, if any, exercising control of the legal person or arrangement through independent sources
c. authorization given for any person to represent the legal person or legal arrangement either by means of Board Resolution or otherwise;
d. where no natural person is identified under the preceding provisions, the identity of the relevant natural persons who hold the positions of senior management;
e. When a legal person's controlling interest is vested with another legal person, the company shall identify the natural person who controls the legal person.
f. Verify if there is an individual/entity who has influence over the account holder, though not a Shareholder/Management personnel.

In order to identify the beneficial owners of a legal arrangement, the company shall obtain and take reasonable measures to verify the following: -

a. For Trusts, the identities of the author of the Trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust, (including those who control through the chain of control or ownership)
b. For other types of legal arrangements, the identities of persons in equivalent or holding similar positions.

Example of Identifying Ultimate Beneficial Owners (UBOs)

As per the above illustration, **AXY Pvt Limited** is the customer.

- Search the UBOs where the ownership proportion is 10% or above with respect of AXY Pvt Ltd.
- As per the above illustration the Ultimate Beneficial Owners are shown in the third layer wherein **Mr. Silva, Mr. Perera, and Mr. Careem** having a **10% and above** control /ownership of the AXY Pvt Ltd

As per FIU guidelines issued on Identification of Beneficial Ownership for Financial Institutions, No 04. of 2018, UBO information is to be obtained as per standard format shown below up to the satisfaction of the company.

Declaration of Beneficial Ownership

a) The following Format "Declaration of Beneficial Ownership" has been circulated with General Circular No 2022/11. The format should be completed when a deposit accounts are opened in our bools (all deposit products)

b) The duly completed format should be filed with the account opening Mandate and made available to competent authorities on request c) Please note that if a prospective depositor refuses to make this declaration Branch Manager should not proceed with the transaction

DECLARATION OF BENEFICIAL OWNERSHIP	
This form has been issued under the Financial Institutions (Customer Due Diligence) Rules, No 1 of 2006 issued in terms of the Section 2 (3) of the Financial Transaction Reporting Act No. 6 of 2006. This form is required to be completed by customers of Financial Institutions designated under the Act to the best of their knowledge. The original completed and signed and witnessed version of this form must be retained by the financial institution and made available to the competent authorities upon request	
Customer Identification:	
Name and Designation of Natural Person opening account	
Name Registered number and address of Legal Person to whom the account is being opened	
Name, Deed Number, Trustee Address of Legal arrangement for which the account is being opened	
I declare that I:	
☐	am the sole beneficial owner of the customer for this account
☐	am not the beneficial owner of the customer for this account. (Complete identifying information for all beneficial owners that own or control 10% or more of the customer's equity, beneficial owners on whose behalf the account is being opened, and at least one person who exercise effective control; of the legal entity regardless of whether such person is already listed)

Definition - Beneficial *Owner is* *"A natural person who ultimately owns or control the customer or the person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement*

Name	NIC No / passport No Country of Issue, Country of Citizenship	Date of birth	Current Address	Source of Beneficial Ownership 1 Equity Indicate % 2 Effective Control 3 Person on whose behalf the account is opened	Check if Politically Exposed Person (PEP)

Details of the Natural person authorized to act on behalf of the Customer / entity
Name
NIC / Passport
Date of Birth
Signature (with seal) By signing you attest to the veracity of all information contained herein and you acknowledge and understand this warning

Verification of Beneficial ownership by an authorized officer of our company	
Authorized Officer of the Financial institution	
Name	
Designation	
Date	
Signature with Seal By signing you attest that you identified the customer whose signature is on this form and witness the said signature	

Ownership

As per Rules 28 and 48, FIs are required to understand the ownership and control structure of their customers when the customer is not a natural person. According to Rule 49, the prescribed threshold for controlling interest is interpreted as owning more than ten percent (10%) of the customer. The ownership could be direct as well as indirect through aggregated ownership as illustrated below.

Figure 1: Simple Indirect Shareholding

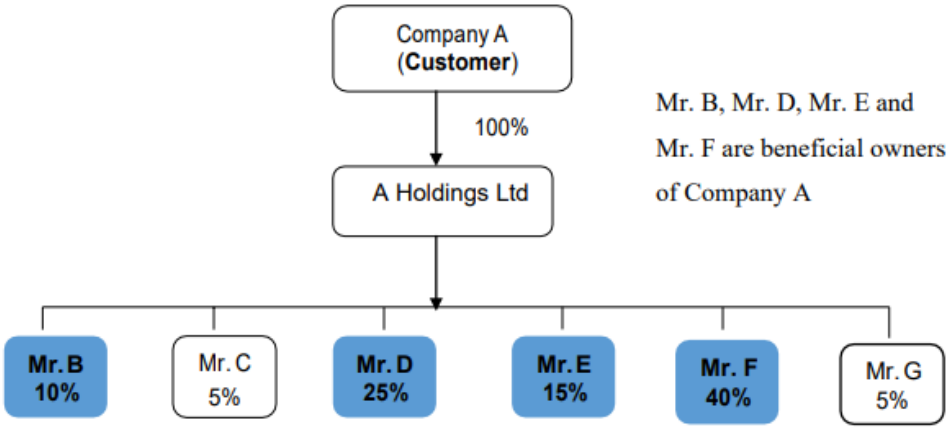
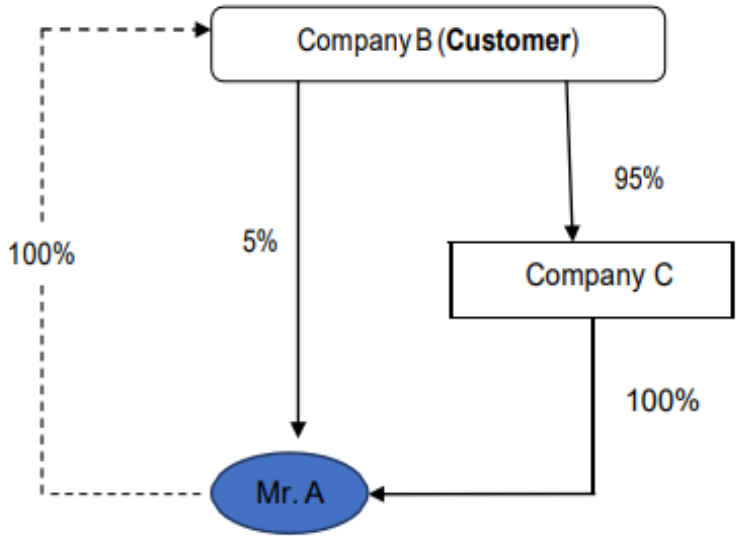
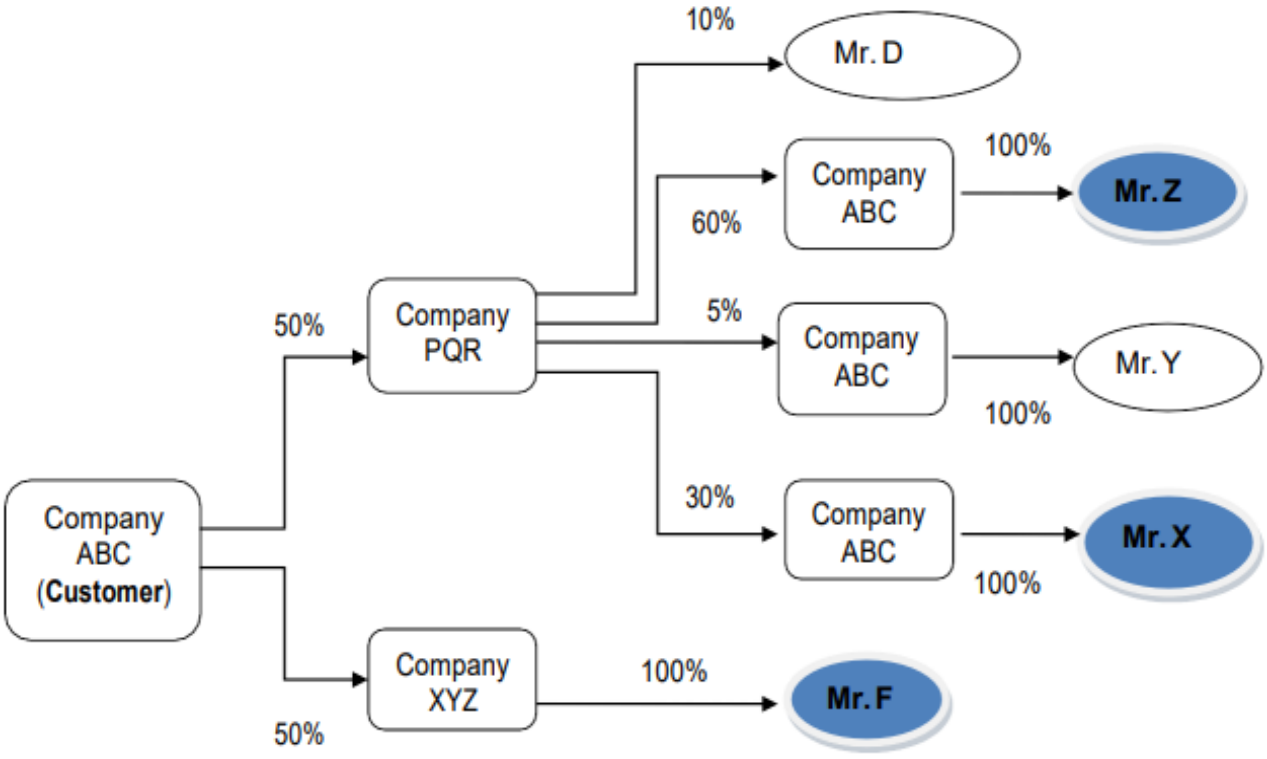


Figure 2: Direct and Indirect Share Holdings



Mr. A is the sole beneficial owner of Company B (Direct 5% + Indirect 95%)

Figure 3: Multi-level indirect shareholdings



Mr. F, Mr. X and Mr. Z are beneficial owners of Company ABC through indirect shareholding

Effective Control

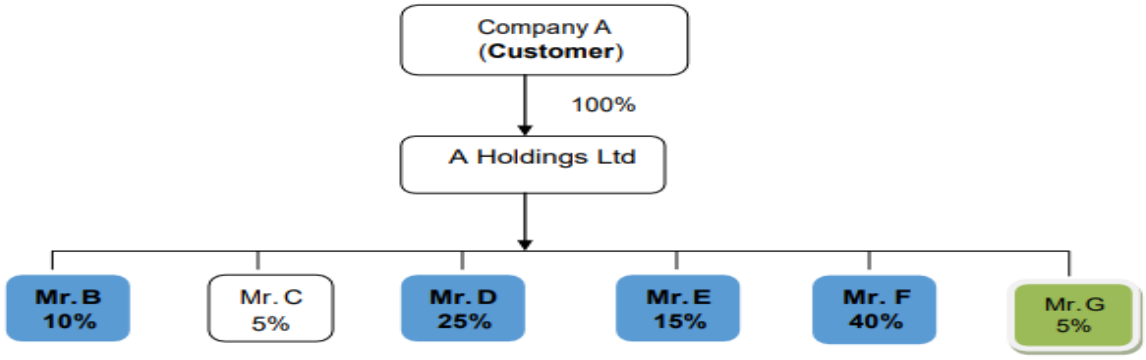
Effective control of a legal person is an important component that determines the beneficial ownership. Such control can be direct or indirect, formal or informal. At a direct and formal level, it is essential to understand the customer's governance structure as an aid in identifying those natural persons that exercise effective control over the customer. In deciding the effective controller(s) in relation to a customer, FIs should consider,

a) A natural person who can hire or terminate a member of senior level management;

b) A natural person who can appoint or dismiss Directors;

c) Senior managers who have control over daily/regular operations of the legal person/arrangement (e.g. a CEO, CFO or a Managing Director).

Figure 4: Effective Control



Mr. G is the managing director of the ABC Bank, which is the main financing source of the company A. In such a situation even if Mr. G holds less than ten percent (10%) of Company A, he has effective control over the company A through ABC Bank and should be considered as a beneficial owner through effective control.

24. REAL TIME MONITORING ACTIVITIES AT BRANCHES THROUGH CLOSED CIRCUIT TELEVISION SYSTEM (CCTV)

- In order to enhance operational risk management and safe guard the Company being abused for money laundering and financing of terrorism, the Company shall have in place a fully operational robust CCTV system installed both within and outside of the premises of the Company such as Head Office, Branches, areas of Automated Teller Machines, Cash Deposit Machines etc.

- The Company shall ensure that CCTV cameras are installed at appropriate locations with adequate lighting in a manner that the camera is able to clearly capture, monitor and record the relevant areas where business operations take place.

- The CCTV systems shall be aligned in a manner and at an angle as to obtain a complete and unimpeded view of the areas where business operations are taking place and the company shall ensure that the CCTV system is not interfered by internal or external lighting, glare or any other object
- Company shall ensure that all images captured visible, recognizable and clear with the capability of identifying the features of the individuals separately. High quality digital equipment with capabilities such as easy viewing, recording and retrieval of high-quality images shall be used by the Company.
- The CCTV systems of ATMs and CDMs shall remain operational throughout 24 hours of a day, every day of the year including the times when the company is closed for business.
- Real time monitoring shall be conducted by the Company and the services of the security services personnel or Law enforcement agencies shall be obtained to mitigate the immediate risk, if such risks are detected.
- The Company shall maintain information captured in the CCTV system for a minimum period of **90days** but shall retain for a longer period if suspicious activities are observed. Further more if instructions are received from Law Enforcement Authorities or any other Competent **Authority the Company shall retain CCTV recordings relevant to a suspicious Transactions Report furnished to FIU until the relevant investigations are concluded.**

25. TRAINING TO STAFF MEMBERS (KYC/ AML/ CFT)

- The Company shall ensure that the training sessions on KYC guidelines and AML & CFT procedures are included in the Training Calendar on an ongoing basis. The company shall arrange to update and modulate these training sessions to the requirements of front-line staff, compliance staff and counter-staff dealing with new customers. It shall be the company's focused endeavour to make all those concerned fully understand the rationale behind the KYC/AML & CFT procedures and implement them consistently.

- The Company's operational staff shall continue to have the conviction to educate and impress the customers that the KYC guidelines are meant for good understanding and for better deliverance of customer service as also for weeding - out the fraudsters in the initial stage itself.

- Transaction monitoring with a view to detect suspicious cases is the most crucial problem that any comprehensive Anti-Money Laundering and Combating Financing of Terrorism measures must address. This fact is effectively taken care of by the structured methodology for implementing KYC/AML & CFT procedures which eventually tend to emit warning signals wherever required and the sustained functional commitment to these procedures in their day-to-day work will enable desk officials to pick-up the adverse signals for reporting to Branch Manager through STR Reports.

26. CUSTOMER EDUCATION

- In order to educate customers on KYC requirements and the need for seeking certain personal information from the customers/applicants for opening accounts and also to ensure transparency, the company shall publish this Policy in the Company's web-site and place a copy of the same in all branches/offices for the reference by user Public.

- It is the duty and responsibility of Operational Staff to educate the customers and tactfully/ convincingly explain the need for customer profile and its relevance in the presentadverse conditions of Money Laundering, Terrorist Financing etc. The customers shall be impressed upon the fact that the profile format enables the branch to render better Customer Service

- An initial resistance by the customers to fill up the exhaustive customer profile format is an expected initial response and it is foreseen as a temporary phenomenon only. The expected resistance could be overcome if the background could be explained to the customers so that the required information can be gathered.

- The Company shall endeavour to guard against denial of financial services to general public especially to those who are financially/socially under-privileged due to the implementation of Customer Acceptance Procedures on too restrictive basis.

27. CONFIDENTIALITY

All employees shall maintain Strict Confidentiality when handling customer documents pertaining to KYC/CDD or personal documents of staff members. It is to be noted that all staff should ensure **No tipping-off** in all such instances where Enhanced Due Diligence measures are carried out for **HIGH Risk customers** including **PEPs** and Suspicious Transaction are Reported to the FIU are based on any suspicion.

28.REVIEW OF POLICY

Both Sections of this policy document should be reviewed annually or as and when the need arises to incorporate new developments and changes and approval should be obtained from the Board of Directors of the company, through BIRMC by the Compliance Department

29. RECOMMENDATION

Recommended to the Board of Directors for adoption

HEAD OF COMPLIANCE **CEO/ EXECUTIVE DIRECTOR**

DOCUMENTS / DATA REQUIRED TO OPEN AN ACCOUNT (A Check List) Attachment 1

Document / Information	Individual Joint accounts	Sole Proprietor Accounts	Partnership Accounts	Corporate Entities	Societies/ Clubs
Account Opening Mandate Format	X	X	X	X	X
Names / Registered Name for Businesses	X	X	X	X	X
Address/ Registered address (Duly Verified)	X	X	X	X	X
NIC with Copy (Unique ID Document)	X	X	All Partners	All Directors	All Office Bearers
Date & Place of Birth	X	X	All Partners)	All Directors	All Office Bearers
Nationality	X	X	X	X	X
Purpose	X	X	X	X	X
Source of Funds / Occupation	X	X	X	X	X
Copy of Registration/ Incorporation		X	X	X	X
Constitution / Memorandum & Articles of Association / Agreements			X	X	X
Resolution / Authority to open account			X	X	X
Income Tax File Number	If applicable	X	X	X	If applicable
Anticipated account turns over per month	X	X	X	X	X
Affiliates/ Subsidiaries / Associates		X	X	X	X
Account Operating Instructions	X If Joint Account)	X	X	X	X
Certificate of Incorporation				X	
Phone / FAX /Email/ Mobile / Web	X	X	X	X	X
Contact Person with NIC			X	X	X
Nominee	X				
Birth Certificate (BC) (use BC number as ID Number)	Podiththa				
Declaration of Beneficial Owner Ship	X	X	X	X	X
Risk Categorization	X	X	X	X	X