Anti -Money Laundering and Combating Terrorist Financing (AML/CTF) Policy

Version Control

Document properties

Owner	Compliance Division
Version	Version 4.0
Review frequency	Annually (as per the CBSL directives)
Document ID	COMPLIANCE POLICY/2024/4.0

Authorization

Drafted by	Compliance Division
Reviewed by	Board Integrated Risk Management Committee
Date	21st September 2023
Approved by	Board of Directors
Date	

Version history

Version	Change reference	Board Approved Date
1.0	Initial Document	27th April 2018
2.0	Review	27th August 2020
3.0	Review	4th June 2022
4.0	Review	
	Effect From	

Distribution and Storage

#	In custody of	Location
1	Compliance Officer	Compliance division

2	Access & Availability	CBSL and every authorised internal/external individual/entity

Contents

List of Abbreviations:

AML	:	Anti-Money Laundering
BIRMC	:	Board Integrated Risk Management Committee
BOD	:	Board of Directors
CFT	:	Cobating Terrorist Financing
CBSL	:	Central Bank of Sri Lanka
CDD	:	Customer Due Diligence
EDD	:	Enhance Due Diligence
FATF	:	Financial Action Task Force
FIU	:	Financial Intelligence Unit
FTRA	:	Financial Transaction Reporting Act
KMP	:	Key Management Personnel

KYC	:	Know Your Customer
ML	:	Money Laundering
NGO	:	Non-Government Organization
PMLA	:	Prevention of Money Laundering Act
PEP	:	Politically Exposed Persons
STR	:	Suspicious Transaction Report
TF	:	Terrorist Financing
UBO	:	Ultimate Beneficial Owners

1. Introduction

Anti -Money Laundering (AML) and Combating Terrorist Financing (CTF) Policy is a guide that sets out the relevant areas that the employees of the Company need to be always aware of. This Policy is issued to enable the 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 noted issued by the Compliance Unit from time to time.

Financial Institutions are facing a heightened level of financial crime threat worldwide. During the past several years, regulatory bodies have been aggressively stepping up their enforcement actions and hence the Finance industry is facing challenges in monitoring the adequacy of control methods utilized to prevent their Financial Institutions being used for such activities.

The Cost of Non-Compliance is very high and the resulted risk, such as the loss of reputation, penalties and monetary loss can be potentially fatal to any Financial Institution. 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 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 Facilities of any forms.

The Board of Directors of Softlogic Finance PLC (SFPLC) believes in good corporate governance both in terms of legal and regulatory compliance. SFPLC is aware that non-compliance with regulatory requirements will expose the Company to reputational, legal and compliance risks which would be detrimental to the profitability and sustainability of the business.

Taking adequate and appropriate steps to combat money laundering and terrorist financing are therefore an integral part of the compliance policy. To fulfil this commitment, a compliance department has been established to provide training for employees in money laundering & terrorist financing prevention practices and controls. The Compliance Department is

responsible for the implementation and monitoring of this program. This Policy sets out the basic legal and regulatory requirements of combating Money laundering and terrorist financing and the Company' policies and procedures on the same. It is an exhaustive document and intended to serve as a reference point for staff in case of any doubts. Sri Lanka has already enacted laws in this respect and the Financial Intelligence Unit of the Central Bank of Sri Lanka has gazetted Know Your Customer (KYC) and Customer Due Diligence (CDD) setting out the procedures for the Financial Institutions, to follow in opening and maintenance of accounts and detecting and reporting transactions of a suspicious nature. This Policy is based on these principles.

2. About this Policy

Coverage	The Policy is applicable to, and used by Softlogic Finance PLC.
Purpose	The purpose of Anti-Money Laundering Policy is to: • Set out the Policies, Procedures and Controls in compliance with the AML/CTF regulatory requirements. • Details the roles and responsibilities of the Company in ensuring compliance with the AML/CTF regulatory requirements; and • Provide guidance on necessary measures and controls to prevent, detect and report potential money laundering and financing of terrorism activities.
Regulatory Requirements	The Policies and Procedures described in the Policy are in line with the Regulatory requirements as detailed in the following Regulations: - • Convention on the Suppression on of Terrorist Financing Act No. 25 of 2005.

	• Prevention of Money Laundering (PMLA) Act No. 05 of 2005 • Financial Transaction Reporting Act (FTRA) Act No. 06 of 2006 • KYC Rules of the Gazette number 1951/13 of 27th January 2016 • Any Regulations pertaining to AML/CFT imposed by CBSL periodically.
Compliance	Non-compliance with AML/CTF regulations imposed by CBSL would result in serious implications not only to the Company but also to respective staff. Therefore, it is imperative that all staff read and understand the policies and procedures of AML/CTF and comply with all the requirements at all times.
Applicability	The Policy shall be read together with other related policies, guidelines, procedures, and standards issued by the Company or regulations issued by the relevant regulatory authorities.
Important	All employees of the Company must strictly adhere to the Policy in carrying out and discharging their duties and responsibilities.

3. What is Money Laundering?

Definition of "Money Laundering"

" The processing of criminal proceeds to disguise their illegal origin in order to legitimize the ill-gotten gains of crime" (FATF).

The Process of Money Laundering

There are, theoretically three factors that are common to Money Laundering operations:

- The real source of criminal money must be concealed and be done without public knowledge.
- The form in which money is held must be changed to hide its identity.
- The trail of transaction must be obscured to defeat any attempted follow-up by law enforcement agencies.

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

In addition to the pervasive threat of money laundering, financial institutions face a significant potential risk associated with the exploitation of their products by terrorist organizations to meet their financial requirements. Recognizing this dual challenge, the Central Bank of Sri Lanka (CBSL) has proactively implemented directives specifically addressing terrorist financing. Consequently, financial institutions are obligated to meticulously comply with these directives to mitigate the risk and ensure the integrity of the financial system.

4. What is Terrorist Financing?

Any person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part for terrorist groups, terrorists or terrorist activities (FATF).

4.1 Different Between Money Laundering and Terrorist Financing

Money laundering seeks to legitimize illegally obtained funds, while terrorist financing aims to fund acts of terrorism. While there may be some overlap in methods and channels used, their primary goals and sources of funds differ significantly.

1. Purpose:
    - Money Laundering: Concealing the illegal origins of funds acquired through various criminal activities.
    - Terrorist Financing: Providing financial support to individuals or groups involved in terrorist acts.
2. Illegal Source:
    - Money Laundering: Involves funds generated from a wide range of illegal activities.
    - Terrorist Financing: Specifically targets funds intended for terrorist activities.
3. End Goal:
    - Money Laundering: Legitimizing unlawfully obtained funds for personal use.
    - Terrorist Financing: Funding acts of terrorism, including planning and execution.
4. Methods:
    - Money Laundering: Utilizes techniques like layering, integration, and placement to obscure the source of funds.
    - Terrorist Financing: Involves directly channeling funds to individuals or groups engaged in terrorism.
5. Focus:
    - Money Laundering: Centers on disguising the origins of money.
    - Terrorist Financing: Focuses on financing activities associated with terrorism.

5. What is Anti-Money Laundering & Counter Financing of Terrorism?

Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) are closely related but distinct efforts aimed at combating financial crimes. **Anti-Money Laundering (AML)** is about stopping criminals from hiding their illegally obtained money and ensuring banks and financial institutions follow rules to verify their customers. **Counter Financing of Terrorism (CFT)** focuses on preventing money from reaching terrorists or terrorist groups. It's a specific part of AML that targets terrorism funding.

In practice, financial institutions and authorities often integrate AML and CFT measures to create a comprehensive approach to combating financial crimes, as these activities can overlap, particularly when terrorist financing involves money laundering techniques to conceal the source of funds.

5.1 Sources of Black Money/Dirty Money

The following are some examples of possible source of black (Dirty) money listed in the 'Prevention of Money Laundering Act. No. 05 of 2006 (PMLA).

- Drug Trafficking
- Arm Trafficking
- Human Trafficking
- Corruption and Bribery
- Participation in Organized Criminal group or racketeering
- Terrorism
- Extortion
- Murder
- Forged or counterfeit currency notes or any legal tender
- Insider Trading and market manipulation
- Damage to property
- Violent Offenses

6. AML/CFT Compliance Governance

Company Responsibilities in 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 Company's Human Resource Department, in line with the Company's Recruitment policy, is to be obtained.

- The Company shall appoint a dedicated Compliance Officer in terms of Section 14 of the FTRA, who shall be responsible for ensuring the 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 is 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.

7. Board of Directors

The Board of Directors (BOD) has the primary responsibility to ensure that the Company complies with all legal and regulatory requirements including those relating to Anti Money Laundering and CTF. Towards this end the BOD has to ensure that a Compliance Officer of sufficient seniority is appointed. BOD will normally delegate the authority and responsibility to oversee this function to the Board Integrated Risk Management Committee (BIRMC).

8. Board Integrated Risk Management Committee (BIRMC)

BIRMC is mandated to establish an independent compliance function aimed at evaluating the company's adherence to laws, regulations, directives, rules, regulatory guidelines, and

approved policies governing its business operations. On an annual basis, BIRMC will conduct a comprehensive assessment of the compliance officer's performance.

The responsibilities of the compliance officer within BIRMC encompass various critical functions. These include:

(i) the development and implementation of policies and procedures to effectively mitigate the risk of regulatory breaches;

(ii) ensuring clear communication of compliance policies and procedures throughout all levels of the organization to foster a robust compliance culture;

(iii) conducting regular reviews at appropriate intervals to evaluate compliance with regulatory rules and internal standards;

(iv) staying abreast of and applying new legal and regulatory developments relevant to the business of BIRMC;

(v) actively participating in the design and structuring of new products and systems to ensure alignment with regulatory requirements, internal compliance, and ethical standards;

(vi) promptly identifying and addressing serious or persistent compliance issues, collaborating with management to rectify them within acceptable time frames; and

(vii) maintaining consistent and positive communication with regulators, founded on transparency and mutual understanding of the regulators' objectives, all conducted with the utmost integrity.

9. Compliance Officer (CO)

It is mandatory to appoint a Compliance Officer who shall be responsible for ensuring the Institution’s compliance with the 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.

9.1 Compliance Officer shall be Responsible For/to

- Develop and implement a comprehensive AML and KYC policy and Customer Due Diligence(CDD) 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 periodically, 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.
- Ensure that AML related mandatory reporting to the FIU is Carried out in accordance with applicable Laws and Regulations.

10. Branch Managers/ Business Unit (BU) Heads/Department Heads

- Branch Managers/BU heads/Department 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.
- Ensure to promptly rectify any irregularities, deficiencies, findings related to the Company/Products/Policies or Procedures identified by the Compliance officer.

11. Staff Members

- Remaining vigilant to the possibility of Money Laundering (ML)/ Terrorist Financing (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 and follow the requirements of the AML/CFT policy on an annual basis.
- Employees are aware that those who violate any of the regulations or the policies/procedures outlined on AML/CFT, will be subject to disciplinary action as per the Human Resource Policy Framework of the Company.

Compliance is Everyone's Responsibility

12. Legal framework for Anti Money Laundering (AML) / Combating ofTerrorist Financing (CTF) in Sri Lanka

For several years government authorities, the Central Bank of Sri Lanka, Financial Sector Authorities and other Legal and Law Enforcement Authorities have worked together with the national experts to formulate the necessary AML/CTF legal framework for Sri Lanka.

The first piece of legislation, the Convention on the Suppression of Terrorist Financing Act, No.25 of 2005 became law on 8th August 2005.

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.

12.1 Prevention of Money Laundering Act (PMLA) No 05 of 2006

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".

Under the Prevention of Money Laundering Act (PMLA) Persons who commit or have been concerned in the commission of predicate offences, and thereby come into possession or controlof property derived directly or indirectly from the commission of such predicate offences will be held accountable and responsible for Money Laundering.

12.2Financial Transaction Reporting Act (FTRA) NO.6 of 2006

The FTRA provides for the setting up of a Financial Intelligence Unit (FIU) as a national central agency to receive, analyze 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 the reporting threshold has been set as amounts Rupees One Million or above (Rs. 1,000,000/-) or its equivalent in any designated foreign currency

The Company's Compliance Department is responsible to collate the report and submit it bi- monthly to the Financial Intelligence Unit of Sri Lanka (FIU). All suspicious transactions need to be reported by the Company to the FIU irrespective of their magnitude.

12.3 Convention on the Suppression of Terrorist Financing 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 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 was further amended under Act no. 41 0f 2011.

Under the Act, the provision or collection of funds for use in terrorist activity with the knowledge or belief that such funds that could be used for financing a terrorist activity, is an offense.

13. Financial Intelligence Unit Guidelines

Rules related to AML/CTF/CDD/KYC etc are made by the Financial Intelligence Unit (FIU) of Sri Lanka.

The first set of rules issued by the FIU were by way of gazette 1951/13 issued on 27th January 2016 and referred to as the "Financial Institutions Customer Due Diligence Rules, No. 01 of 2016.These rules were issued under Section 2 of the Financial Transactions Reporting Act No.6of 2006 and any contravention of, or non-Compliance with the same will be liable to the penalties under the relevant provisions of the Act.

The FIU further issued a guideline via Circular No 1/18 with Ref: 037/05/002/0018/017 dated 11th January 2018 referred to as "Guidelines on Money Laundering and Terrorist Financing Risk Management for Financial Institutions No 1 of 2018", the Identification of Beneficial Ownership of Legal Persons who are customer's of the Company by way of Guideline 037/07/006/0004/018 (Guideline 04/2018) dated 19th April 2018.

Further emphasis on the requirement to report suspicious transactions to the FIU and guidelines on how to do so, were issued by the FIU on 06th August 2018 by way of "Guidelines for Financial Institutions on Suspicious Transaction Reporting No 6 of 2018" with reference No. 037/03/011/0001/018. A further Direction on the conducting of Due Diligence on NGOs, NPOs

and Charities was issued on 23rd May 2019 where it was made mandatory for all International and National level foreign funded voluntary social service organizations/NGOs to re-register with the National Secretariat for Non Governmental Organizations. New guidelines on the identification of Politically Exposed Persons (PEPs) was issued by the FIU on 1st October 2019 under reference 037/07/006/0013/018 which covered aspects relating to the identification of PEPs and managing of Risk pertaining to such business relationships. Clarification on managing Debit frozen Accounts in Financial Institutions was issued by the FIU on 3rd December 2019 by way of circular 02/19 caring reference 37/02/008/0016/016. Following the covid19 pandemicand the increase in digital transactions, the FIU issued a guideline to the Financial Institutions on 15th June 2020 under reference 037/02/008/0010/016 requesting the Financial Institutions to be vigilant to emerging ML/TF risks.

The Guidelines for Non-face- to- face Customer Identification and Verification Using Electronic Interface provided by the Department for Registration of Persons, No. 03 of 2020 was issued in 2020, in order to strengthen the procedure of onboarding non-face-to -face customers.

The Guidelines for Financial Institutions on CCTV Operations for AML/CFT purpose, No. 02 of 2021 was issued in 20

14. Customer Due Diligence

The Company and its branches must conduct Customer Due Diligence (CDD) and obtain satisfactory evidence and properly establish in its records the identity and legal existence of any person applying to do business with it. The Company should not commence any business relationships or perform any transaction, or in the case of existing business relationship, it should terminate such business relationship, if the customer fails to comply with the CDD requirements and consider lodging a suspicious transaction report with the Financial Intelligence Unit in Central Bank of Sri Lanka.

14.1 CDD must be conducted in the following events:

- At the point of establishing business relationships with any customer.
- When a customer is carrying out cash transactions that is not in line with its risk profile.
- When there is any suspicion of money laundering or financing of terrorism.
- When there is any doubt about the veracity or adequacy of previously obtained information.
- Any change of personal information given previously
- Activating dormant accounts, if the Company has any suspicion of money laundering or financing of terrorism activities, CDD must be conducted on the customer, including the person conducting the transaction, regardless of the amount transacted.

14.2 CDD should at least comprise the following:

- Identify and verify the customer

- Identify and verify beneficial ownership and control of such transaction
- Obtain information on the purpose and intended nature of the business relationship/transaction
- Conduct on-going due diligence and scrutiny to ensure the information provided is updated and relevant.
- The unwillingness of the customer to provide the information requested and to cooperate with the Company's CDD process may itself be a factor of suspicion.

As part of ongoing CDD, the Company should take reasonable measures to ensure that the record of existing customers, including its risk profile, remains updated and relevant. In addition, further evidence in identifying the existing customers should be obtained.

15. In addition to CDD, for higher risk customers, the Company must also conduct Enhanced Due Diligence (EDD). Some examples of higher risk customers include:

- High net worth individuals
- Non-resident customers
- From locations known for high rates of crime (e.g. drug producing/trafficking/ smuggling);
- Countries or jurisdictions with inadequate AML/CTF laws and regulations such as the Non-Cooperative Countries and Territories.
- Local and Foreign Politically Exposed Persons (PEPs)
- Legal arrangements that are complex (e.g., trust, nominee)
- Cash intensive businesses
- Businesses/activities identified by the FATF as of higher money laundering and financing of terrorism risk.

Reference: For details, refer to AML/CFT Guidelines on Risk Assessment & Monitoring of Higher Risk Customers/Transactions.

EDD should include at least: Obtaining more detailed information from the customer and through publicly available information, in particular on the purpose of transaction and source of funds; and Obtaining approval from the Senior Management of the Company before establishing the business relationship with the customer.

15.1 Non-face -to face Business Relationships

The Company may establish non-face to-face business relationships in line with the relevant regulatory guidelines and EDD process. All customer relationships established through non-face-to-face channels must be considered and rated as high risk.

16. Identifying Ultimate Beneficial Owners (UBO)

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 is to determine that 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.

17. KYC/CDD for Legal Persons and Legal Arrangements

1. If a customer is a legal person or legal arrangement, The Company shall,
    a. Understand the nature of the customer' s business, its ownership and control structure;
    b. Identify and verify the customer in terms of the requirements.

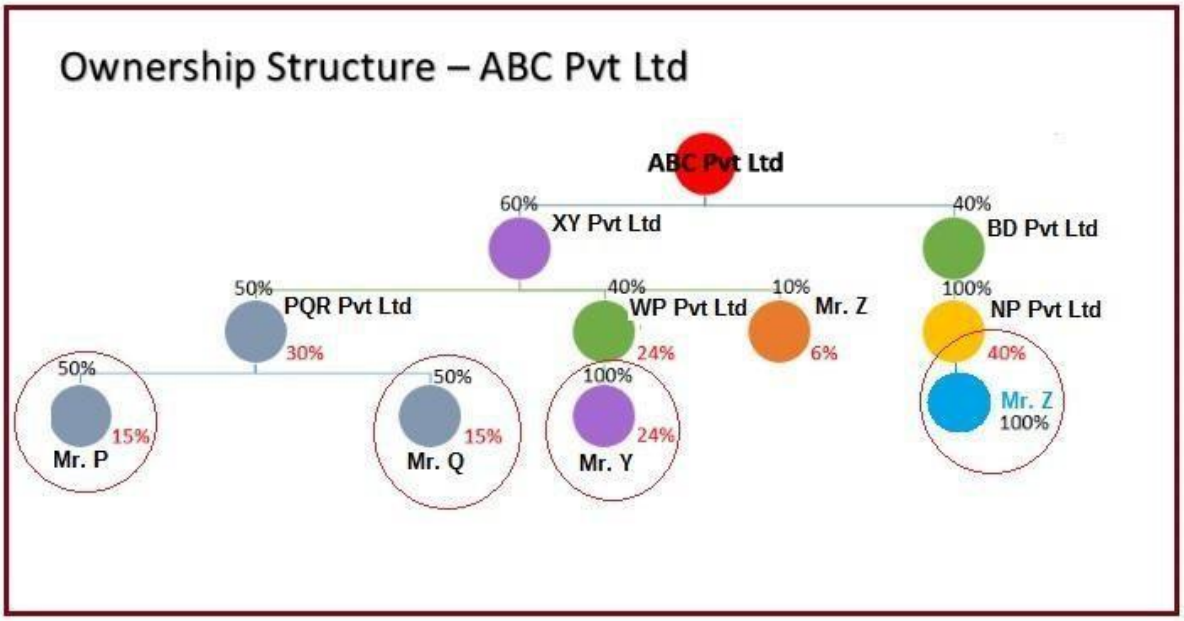
2. In order to identify the natural person (UBO) if any, who ultimately has controlling ownership interest in a legal person, the Company at the minimum shall obtain and take reasonable measures to verify the following:-

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 identityof 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.

3. 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.

17.1 Example of Identifying Ultimate Beneficial Owners (UBOs)



As per the above illustration, **ABC Pvt Limited** is the Company Customer.

- Company need to search the UBOs where the ownership proportion is 10% or above with respect of ABC Pvt Ltd.
- As per the above illustration the Ultimate Beneficial Owners are shown in the third layer wherein **Mr.P, Mr. Q, Mr. Y and Mr. Z** having a **10% and above** control/ownership of the ABC 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 FI.

Declaration of Beneficial Ownership	
This form has been issued under the Customer Due Diligence Rue No 1 of 2016 issued in terms of the Section 2(3) of the Financial Transactions Reporting Act of 2006. This form, or an approved equivalent, is required to be completed by all customers of financial institutions designated under the Acts 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 available to the competent authorities upon request.	
Customer Identification:	
Name and Designation of Natural Person Opening Account	
Name, Reg. No. and Address of Legal person for Which the Account is Being Opened	
Name, Deed No., Trustee and Address of Legal arrangement for Which the Account is Being Opened	
I declare that I:	
☐	am the beneficial owner[2] of the customer for this account.
☐	am not the beneficial owner[2] of the customer of 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 operated, and at least one person who exercises effective control of the legal entity regardless of whether such person is already listed.

2 Beneficial owner as "a natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a person or a legal arrangement."

Name	NIC or Passport # /Country of Issue/Country of Citizenship	DOB	Current Address	Source of Beneficial Ownership (1=Equity (indicate %), 2=Effective Control, 3=Person on Whose Behalf Account is Operated)	Check if Politically Exposed Person (PEP) [3]
					☐
					☐
					☐
					☐

Details of the Customer Authorized to Act on Behalf of Entity
Name :
NIC/Passport :
Date of Birth :
Signature and Company Seal: (By signing you attest to the veracity of all information contained herein and you acknowledge and understand the above warning)

Verification of Beneficial Ownership

Cargills Bank Authorized Official
Name :
Title :
Date :
Signature and Seal: (by signing, you attest that you have identified the Customer whose signature is on this form and have witnessed said signature)

3 Politically exposed person" means an individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a Head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a State owned Corporation, Government or autonomous body but does not include middle rank or junior rank individuals

17.2 Identification and Verification of Beneficial Ownership Information

- The Company should obtain information to identify and take reasonable measures to verify the identity of the Beneficial Owner(s) of the customer using relevant information or data obtained from a reliable source, adequate for the Company to satisfy itself that it knows who the Beneficial Owner(s) is.

- Accordingly, the identification of UBO is mandatory. Once the Company establishes who the UBO(s) of a customer is/are, the Company must collect at least the following information in relation to each individual Beneficial Owner:

  a) Full name
  b) Official personal identification or any other identification number
  c) Permanent/ Residential address.

- The Company staff can rely on verifying Beneficial Ownership, through the following documentation (but not limited to):

  a) Share register,
  b) Annual Returns,
  c) Trust deed,
  d) Partnership agreement,
  e) The constitution and/or certificate of incorporation for an incorporated association,
  f) The constitution of a registered co-operative society,
  g) Minutes of the board of directors meetings,
  h) Information available through open-source search or commercially available databases.

Valid Identification Document of UBOs is to be obtained at the point of Account opening and is required to be retained along with the mandates of the Legal Person.

- In case of foreign legal persons and arrangements, the Company may also have to take additional measures such as verification through mother company or branches, correspondence Company, other agents of the Company, corporate registries etc.

- 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 UBOs, the Company can use relevant identification information available from reliable sources (e.g. a public register) to identify the Directors and major Shareholders.

- The Company staff have to identify the natural persons holding Senior Management positions as Beneficial Owners when the Company is unable to determine the UBOs as there is no person owning more than 10% (ten percent) of the customer's equity or no individual exercising control over the customer.
- Declaration of Beneficial Ownership by the customer

Effective Control

In deciding on the Individuals who have Effective Control in relation to a Legal Person the Company should consider the following.

- A Natural Person who can hire or terminate a member of Senior Level Management
- A Natural Person who can appoint or dismiss Directors
- Senior Managers who have control over daily/regular operations of the legal person/arrangement (e.g. a CEO, CFO or a Managing Director).

Customer Due Diligence – Basic Identification Information Verification – Opening of Accounts

Basic identification information verification should be carried out for opening of accounts for the following types of customers:-

- Natural person (i.e., individual)
- Partnerships/Sole Proprietorships
- Corporate entities
- Clubs /Societies/Charities/ Associations and NGO's
- Trusts Nominees and Fiduciary accounts
- Minors

The following table shows the Regulations relating to KYC/CDD requirements at the time of opening accounts. The information must be reviewed and kept updated at regular intervals and at any time a necessity arises to verify the accuracy of the information.

Natural Persons

Basic Information Required	Verification Methods
Full Name	• Sight Original Document • Confirming the Permanent Address (e.g. Utility Bill, Tax Assessment, Bank Statement, a letter from a public authority, certificate from Grama Niladhari, or electoral register. • Contacting the customer by telephone/ letter to conform the information supplied after and account has been opened (e.g. disconnected phone, returned mail or incorrect email address should warrant further investigation) or conduct a field visit. • By reference to Birth Certificate or Original NIC. • Confirming the Nationality, for foreigners, taxpayer identification, passport or any other government issued document evidencing nationality or residence should be obtained
Male/Female	
Permanent Address (Full address should be obtained)	
Telephone/Fax/Email	
Date and Place of Birth	
Nationality/Citizenship	
An Official Personal Identification Number or any other identification number (NIC, Passport, Driving License) that bears a photograph of the customer	
Occupation type/self employed	
Public Position held	
Name of Employer/Nature of the employment/nature of business	
Purpose of Account Opening	
Source of Income	
Expected Turnover/Volume of Business	

Documents to be obtained

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

- Mandate/Account Opening form.
- KYC Form
- Copy of identification document.
- Copy of address verification documents.
- Copy of the valid visa/permit in the case of non-nationals.
- Copy of the business registration if the account is opened for such purpose.

Sole Proprietorship and Partnership

In the case of a partnership, the Company shall verify the identity of each partner of such partnership and also verify the details of immediate family members who have ownership or control thereof.

The following table shows the Regulatory requirements on KYC and CDD for Partnerships.

Basic Information Required	Verification Methods
• Full name as appearing in the Business Registration document • Personal details of the proprietor/partner as in the case of individual accounts. • Registered address or the principle place of business • The permanent address of the proprietor/partners • Contact telephone, fax numbers and emails • Nature and purpose of business. • Tax file number • Satisfactory references • Signatures • The extent of the ownership controls • Other connected business interests	• By reference to Business Registration Certificate • By reference to Birth Certificate, NIC, Passport etc of the Proprietor/partners • Contacting the corporate entity by telephone, mail or e-mail • Name Screening • CRIB • Other Bank's reference

Documents to be obtained

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

- Mandate/Account opening form
- KYC Form
- Copy of the business registration certificate
- Copy of identification and address verification documents of proprietor

Corporate Entities

The following table shows the Regulatory requirements on KYC and CDD for Corporate Entities (incorporated companies).

Basic Information Required	Verification Methods
• Registered name of the institution. • Principal place of institution's business operations • Mailing address • Telephone/Fax/E-mail • Nature and purpose of business • Income Tax file number • Bank references • Personal details of all Directors as in the case of individual customers • Major shareholders and their financial interests and control • List of subsidiaries/associates and other business connections • Signatures • Registered address	• By reference to Certificate of incorporation • By reference to certified copy of form 13 • where possible utilising an independent information verification process, such as by accessing public and private databases visiting the corporate entity, where practical • Contacting the corporate entity by telephone, mail or e-mail • By reference to Articles of Association • By verifying with the Bank issuing reference • By reference to Form 1 and/or form 20 (Certified copy issued by Registrar of Companies) • By reference to Last Annual Return/Annual Report and also certificate issued by the Company Secretary (updated information) • Identify all owners of companies/firms • Name Screening • CRIB Report

Note: The non-documentary methods 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. Where there is any doubt:

• Conduct a basic search or enquiry on the background of such company/business to ensure that it has not been, or is not in the process of being, dissolved or liquidated; and

• Verify the authenticity of the information provided by the company/business with the Records maintained at Department of Registrar of Companies

Clubs, Societies, Charities, Associations and NGOs

Societies and Cooperatives

In the case of societies and cooperatives the principal shall be those exercising control or significant influence over the organization's assets. This will often include board members and executives and account signatories.

Charities, Clubs and Associations

In the case of charities, clubs, and associations the company has to take reasonable steps to identify and verify at least two signatories along with the institution itself. The principal shall be those exercising control or significant influence over the organization's assets. This will often include members of a governing body or committee, the President/Chairman, the members of the Board of Directors, or managing body, the treasurer, and all signatories. In all cases independent verification shall be obtained that the persons involved are true representatives of the institution.

In all cases independent verification shall be obtained that the persons involved are true representatives of the institution. The following table set out the KYC/EDD requirements specified by Regulations.

Basic Information Required	Verification Methods
• Registered Name and the Registration Number of the institution • Registered address as appearing in the Charter, Constitution etc. • Detailed information 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. • The purpose for which the account is opened, the objectives and the areas of activities. • The source and level of income/ funding. • Other connected institutions/ associates/organizations. • Telephone, Facsimile numbers and email address. • In case of NGO's etc verify that they are duly registered with the National Secretariat for NGOs	• By reference to the registration Documents • EDD as applicable to individual accounts. • Closely scrutinise the accounts of clubs, societies or charities in order to detect discrepancies in the transactions and account activities.

Documents to be Obtained

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

- Copy of the registration document/constitution, charter etc.
- Customer information form as in the case of individual accounts.
- Mandate/Account Opening Form.
- KYC Form

Trusts, Nominees and Fiduciary Accounts

The Company shall take reasonable steps to verify the trustee, the settler of the trust (including any persons settling assets into the trust) any protector, beneficiary, and signatory In the case of a foundation, the Company shall verify the founder, the managers, directors and the beneficiaries.

Basic Information Required	Verification Methods
• Identification of all trustees, settlers/grantors and beneficiaries in case of trustees • Whether the customer is acting as a 'front' or acting as a trustee, nominee, or other intermediary.	• Verification methods applicable to Individuals and corporate are applicable here as appropriate.

Documents to be Obtained

- Mandate/Account Opening Form
- Copy of the Trust Deed
- Particulars of all individuals
- KYC Form

Responsibility for Conducting Customer Due Diligence

Responsibility within the Company for conducting the Customer Due Diligence rests with the respective staff member who opens the account and manages the relationship, retains primary responsibility for the customer relationship and KYC requirements.

Prohibited Businesses /Relationships

The Company has zero risk appetite for following business types and is prohibited to open or maintain such relationships.

- The Company shall not establish an anonymous account, numbered account, account in a fictitious name.
- The Company shall not establish business relationship with a person or entity refusing to provide information and documentation that are subject to due diligence.
- Entity where ultimate beneficial owners (UBOs) cannot be identified.
- Entity or individual listed in national or international Sanctions lists (SDN). Entity or individual resident in a comprehensive Sanctioned jurisdiction identified by FIU.
- Business prohibited by regulations or law (Eg illegal betting/gambling centres,Adult/red light business, unregulated charities/money service businesses, Virtual currency related businesses etc).
- Shell Companies.

Definitions of Customer Types

"Occasional Customers" means as per section 2(6) of the FTRA defines Occasional transactions as any transactions, in relation to cash and electronic fund transfer that is conducted by any person other than through an account in respect of which the person is the customer.

"One-off Customers" means customers who do not access their account maintained at the Company on a regular basis for financial transaction either physically of from an online account platform access to which is provided by the Company.

"Walk-in Customers" means a person who is not a customer of the Company to which he has presented himself although the purpose of his visit is to obtain a financial service or to conduct a financial transaction with such institutions.

Third Party Deposits

With regard to all cash deposits exceeding Rs. 200,000/- (Rupees two hundred thousand) made into an account separately or in aggregate by a third party customer, it is required to record the name, address, identification number of a valid identification document, purpose and the signature of the third party customer. The information noted on the voucher needs be legible and available for future reference is require.

Provided however where, 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 for this purpose:

"Third Party Customers" means a person who transacts with a company through a Third party accounts in respects of which the third party is the customer of such Company Provided that, 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.

Customer Risk Profiling

All Companies are required to perform **Risk Based Compliance**. Risk profiling of all customers is mandatory and is to be done by way of the information derived by the Company through the KYC and Customer Due Diligence (CDD) process.

Where any customer is rated as "**High Risk" the Company is required to carry out Enhanced CDD measures**, in addition to the normal CDD measures undertaken.

The Company has developed a Risk Matrix to enable the branches/frontline staff to ascertain particular AML Risk Profile (Low, Medium of High) of a given customer.

A Brief description of Low, Medium, and High-risk categories is given below.

The profile will be evaluated taking the following into consideration

- Low Risk

Individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as Low Risk.

The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover. E.g.: Student /House wife/Pensioner/farmer.

Recommended frequency for periodical review: Every Five Years or upon a trigger.
Delayed Verification can be done for Low-Risk Customers subject to the below.

Delayed Verification process

- Verification shall be completed as soon as it is reasonably practicable but not later thanfourteen (14) working days from the date of opening of the account.
- The delay will be essential so as not to interrupt the Company's normal conduct of business.
- No suspicion of money laundering or terrorist financing risk shall be involved with the customer.

- Medium Risk

Customers who are likely to pose a higher than average risk to the Company may be categorized as Medium or High Risk customer, depending on the customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Such as:

- Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful and not all information is immediately verifiable.
- Fund flow sources not well documented or known to the Company or verifiable immediately; deposits to the account frequently exceed the declared income threshold by the customer; with adequate /known reasons.

- Recommended frequency for periodical review: Every Three Year or upon a trigger
- Delayed Verification: Delayed verification is not permitted for Medium Risk Customers.

- High Risk

The Company will be required to apply Enhanced Due Diligence measures based on the risk assessment, thereby requiring intensive 'Due Diligence' for Higher Risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher level of Due Diligence may include.

- Non Resident Customers,
- High Net worth individuals
- Trusts, charities, NGOs and organizations receiving donations,
- Companies having close family shareholding or beneficial ownership
- Politically Exposed Persons (PEPs) of foreign/local origin
- Non-face to face customers, and
- Those with dubious reputation as per public information available, etc.

- Recommended frequency for periodical review: at least annually or more frequently on a trigger basis.
- Delayed Verification: Delayed verification is not permitted for High Risk Customers

Note:- If a customer opens accounts/or creates any other business relationships with the company after 6 months of obtaining the initial KYC details, a new KYC form should be completed, in order to capture significant changes to the initial KYC details. This process should be ensured every six months, when a customer enters into new facilities/business relationships.

Periodic Reviews

Conducting of periodic review includes the following in the case of Legal Persons

1. Relevant KYC Review Form to be obtained.
2. Director KYC to be reviewed
3. UBOs of the Entity to be reviewed and the Core System updated accordingly (Documents to verify identification of changed UBOs to be obtained).
4. Name Screening to be conducted on the Entity, its Directors, UBOs and any other connectedparties.

5. Entity, Director's and UBOs Risk Ratings to be revised and the core system to be updated accordingly
6. KYC Review dates to be updated in the core system.

Conducting of periodic review includes the following in the case of Natural Persons

1. Updated KYC Form to be obtained and supporting documents to be obtained for any changes(includes clarification on PEP status)
2. Risk Rating to be revised and the system to be updated accordingly
3. Name Screening is to be conducted
4. Ensure that valid identification document is retained.

All documents used for the review to be retained in the relevant customers file

Strict Confidentiality

The Risk Profiling and the resultant information are exclusively for Company's internal use only and is usedfor the purpose of mitigating the ML/TF risk posed to the Company. **Strict confidentiality must be maintained at all times. The customer should NOT be informed of his/her Risk Profile** under any circumstances.

Politically Exposed Persons - PEPs

A PEP is an individual who is entrusted with prominent public functions either domestically or by aforeign country, or in an international organization and includes a Head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a State owned Corporation, Government or autonomous body but does not include middle rank or junior rank individuals.

Immediate family members of PEPs include any of the following relations, who should also be identified as PEP in addition to the close associates as well.

i. Spouse (current and past);

ii. Siblings, (including half-siblings) and their spouses

iii. Children (including step-children and adopted children) and their spouses;

iv. Parents(including step-parents); v. grand children and their spouses.

A Close Associate means,

- A natural person having joint beneficial ownership of legal entities and legal arrangements,or any other close business relationship with a PEP/family member.
- A legal person or legal arrangement whose beneficial owner is a natural person and is known to have been set up for the benefit of such person or his immediate familymembers.
- A PEP's widely- and publicly-known close business colleagues or personal advisors, in particular, persons acting in a financial fiduciary capacity.

1. This category of customers known as PEPs and are required to be categorized as HIGH Risk from an ML Compliance perspective. However regulatory guidelines **do not prohibit** dealings with PEPs. But **Enhanced Due Diligence (EDD)** is required to be carried out on such customers.

2. The Account opening staff are required to obtain approval from the Senior Management. Copies need to be retained along with the mandate and other account opening documents of the customer.

3. For those identified as PEPS the Company should identify, by appropriate means, the sources of funds and wealth or Beneficial Ownership of funds and wealth and be fully satisfied of the legitimacy of it as part of EDD process

4. Be fully satisfied that the Customer does not expose the Company to unacceptable levels of ML/TF risk.

18. Using New Technologies

The Company must identify and assess Money Laundering and Terrorist Financing risks that mayarise 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.

The Company must ensure that compliance sign off is obtained and -

- Undertake the risk assessments prior to the launch or use of new products, practices andtechnologies
- Take appropriate measures to manage and mitigate the risks which may arise in relation tothe development of new products and new business practice.

19. Suspicion Transaction/Business

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, personal activities or with the normal business for the type of account created.

The following are some, but certainly not all areas where staff should remain vigilant to possible Money Laundering situations. The fact that any of the following do occur does not necessarily lead to a conclusion that Money Laundering has taken place, but they could well raise the need for further enquiry. A key to recognizing suspicious transaction/transaction patterns is to know enough about the customer to recognize if they are unusual for that particular customer.

While the following provide some examples, recognizing suspicious transactions is a matter of good sense and attention to detail by all staff of the Company.

Suspicious Cash Transactions

- Unusually large cash deposits made by an individual or a company.
- Substantial increase in cash deposits by any customer 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.
- Frequent third-party cash deposits to the account.

- Large cash withdrawals from a previously dormant/inactive account.

Suspicious Transactions using Customer Accounts

- Customers who maintain a number of trustee or customers' accounts which are not required by the type of business they conduct particularly.
- Customers who have accounts with several financial institutions within the same locality and who transfer the balances of those accounts to one account .
- A large number of individuals who deposit monies into the same account without an adequate explanation.

Suspicious Loan Transactions

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

Recognizing and Reporting of Suspicious Transactions

In accordance with the local Laws and regulations it is an offence to fail to report suspicion of Money Laundering and/or Terrorist Financing. Failure to report such circumstances is punishable on conviction for heavy fines and/or imprisonment.

Reporting Procedures

Reporting the Suspicious Transaction to the Compliance Department

Any staff member who identifies a suspicious transaction/customer should report the same to the Company's Compliance Department.

Role of the Compliance Officer on receiving the Report

When the Compliance Officer receives the Suspicious Transaction Information, the Compliance Officer will conduct further Due Diligence and decide whether the report gives rise to knowledge or suspicion that customer is involved in Money Laundering or Terrorism Financing.

If the Compliance Officer believes that the suspicions may be justified and requires further investigation, it must be reported to the Financial Intelligence Unit (FIU) within 2 working days.

The importance of timing

It is very important that there is no delay in reporting. It is the duty of all employees to report suspicion as soon as they have established reasonable grounds, and collected the relevant supporting material.

In accordance with the circular issued by the FIU, the compliance officer is required to assess the urgency of FIU requests and ensure the timely submission of the report within the specified timeframe.

Extremely Urgent – Within 24 hours
Urgent – Within Three (3) working days
General Requests – Within Two (2) weeks

Tipping Off

Duty of the staff members reporting the suspicion or those aware of the suspicion is not to divulge information to other members of staff or any others including the respective customer/entity and report only to the Company's Compliance Officer or his/her designate.

The Company will protect persons reporting suspicious transactions if done in good faith and compliance with regulations under the Applicable Laws and Regulation and Directions of FIU, issued from time to time.

The Financial Transaction Reporting Act (FTRA) makes "tipping-off" an offence under the Act (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.

Under no circumstances should the customer know that they have been reported for the activity, or that an investigation is underway or may be underway.

This does not mean that the Company cannot ask the customer for an explanation or continue to provide them with a normal customer service. But it does mean that the Company must do so without alerting them to the fact that the Company may or had already notified the Authorities of suspicion on the transaction carried out by him/her or the entity.

20. Freezing of accounts/Transactions

Time to time, the Company may be required to freeze accounts or transactions of customers based on explicit request of regulators including the FIU.

Company staff should act promptly to such requests without fail and should not remove/amend accounts under freeze without explicit instructions received from regulators.

Compliance Department should be kept aware of any action related to an account/transaction frozen/blocked related to AML/CTF received from Regulators.

21. Sanctions and Name Screening

The Company is subject to the provisions of various Sanctions programs administered.

The Company needs to be in compliance with all Directions issued by the FIU on complying with UNSCR, OFAC, UN, EU and all other globally, mandated sanctions lists. Responsibility within the Company for checking names against sanctions lists or similar restrictive measures rests with the respective Branch/Departments using the screening system subscribed by the Company.

Name screening is the process of determining whether any of the Company's customers (new and existing), are part of any regulatory black lists. In the event of the Company's customer or the persons with whom they deal with match any of the listed individuals or entities on the watch list/blacklist, the Company is required by way of regulation to investigate, monitor and where required to report such matches to the designated authority,

To comply with this, the Company has taken the steps to implement an automated Name Screening System against the sanctioned lists.

22. Independent Audit Testing

Company has entrusted Internal Audit Department with the responsibility to test the implementation and adherence of the Company's KYC/AML Policy. This examination is required to be conducted as part of the audit plan of the Internal Audit Department. The findings/recommendations should be reported directly to the Board Audit Committee.

23. Compliance Monitoring and Testing

The Compliance Department also carries out reviews and testing to verify among other things the implementation and adherence of the AML Policy and related circulars in the Company and report any non-Compliances to the Board. The reviews are conducted as per the BIRMC approved compliance programme/plan.

The Compliance function shall monitor and test Compliance by performing sufficient and represented testing based on a Risk methodology adopted. The reports should be submitted to the BIRMC.

24. Record Keeping Obligations

In addition to regular Company record keeping requirements, the Company's policy under Money Laundering requires that documents concerning customer identification and records relating to transactions undertaken on behalf of customers/non-customers, be maintained for a period of 6 years from the closure of the account enabling to provide a clear audit trail in the event of an investigation.

It is also required that: -

- All Anti-Money Laundering monitoring reports made by the Compliance Officer and records of consideration on those reports and of any action taken as a consequence including reporting done to management/auditors/regulators be maintained for a 6 year period for future reviews.
- All records maintained should be available to authorized persons promptly on request

without undue delays.

25. Dissemination of New Laws and Regulations

All New Directions and Regulations Received by the Company pertaining to AML/KYC and CDD would be received by the Head of Compliance/Compliance Department without delay. These are then required to be forwarded to the applicable respective Business Unit/Department Heads for further action. The Head of Compliance shall also include the new laws and Directions amendments as part of the Monthly Compliance Board Papers, for the information of Board members.

26. Training to Staff members (KYC/ AML/CDD)

Compliance shall ensure that the training sessions on KYC guidelines and AML procedures are included in the Training Calendar on an ongoing basis for all staff.

Branch Managers and Heads of Department should additionally 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.

27. Guidelines For Financial Institutions on CCTV Operations for AML/CTF Purposes

A Closed-Circuit Television (CCTV) system allows the use of video cameras to monitor the interior and exterior of a property, transmitting the signal to a monitor or set of monitors. The primary purposes for the use of CCTV surveillance technology are to deter crime, investigate crimes and policy violations and identify involved parties. It also serves the purpose of evidence to the law enforcement authorities in their investigations.

As a part of constant commitment to enhance operational risk management and safeguard financial operations against risks of being abused for money laundering and financing of terrorism, Softlogic Finance PLC shall have in place a robust CCTV system installed fully operational both within and outside the premises. The premises refer to head office, branches, areas of Automated Teller Machines, Cash Recycling Machines and Cash Deposit Machines (ATM/CRM/CDM), cash centers, outlets and any other

place or places where Customer Due Diligence (CDD) is conducted. The company adheres to the FIU guidelines by retaining and securely storing all CCTV footage records for a duration of 90 days.

28. Guidelines on responsibilities of the Financial Institution with respect to Suspension And Extension Orders

Guidelines on Suspension of Transaction for FIs

Responsibilities of the Financial Institution (FI) with respect to suspension and extension orders:

i) On receipt of the suspension orders the Compliance Department will acknowledge the receipt of the orders and check whether the individual / entity maintain any relationships with the company and obtain confirmation from the Operations Department.

ii) If the individual / entity maintains any relationships the Compliance Department will inform the relevant departments (Operations, FD Operations, Leasing, Factoring, other) to place suspension on the accounts and freeze all debit transactions on the account. If there are no relationships with the said parties, instructions would be provided to the relevant unit to block the customer in the system.

iii) The respective departments (Operations, FD Operations, Leasing, Factoring, other) will confirm immediately placing of the suspension order and freeze all debit transactions and will also provide information on all business relationships maintained by the concerned individual / entity including connected any connected business relationships and the nature of to the Compliance Dept. with balances available in the account as at the date of suspension. Upon the confirmation from the respective departments, the Compliance Dept will inform the FIU accordingly.

iv) Communicating the suspension order to customer: - The respective business unit may inform the customer about the suspension of his / her transactions only upon an inquiry by the customer and in the same manner the inquiry is made The business unit is not required to provide reason sfor such action by the FIU to the customer. In relation to extension of suspension, the business unit may inform the customer that funds / accounts / transactions have been suspended as per an order of the High Court of the Western Province holden in Colombo. The business unit should take

prudent steps only to provide information that is necessary in the communication process to the customer.

The FI shall flag every individual and institution subjected to a suspension order as 'HIGH RISK' customers.

29. Breach of policy

Failure to abide by the Company AML /CTF policy leads to loss of confidence in the Company's integrity and fair dealing, severe impact on the Company shareholders, customers, and the relevant regulatory bodies, market, and significant adverse publicity and reputational damage, even if no law was broken. As a result, management will take appropriate corrective action in the scope of laws, policies and procedures when breaches of laws, rules and standards are identified that might include "Disciplinary Action", and "Termination of Employment".

30. Communication of Policy

The Policy will be published on the Company's Intranet and would be circulated to all staff notifying that the Policy has been reviewed and updated and that all staff are required to read and understand the contents there of.

Note:- In the case of any inconsistency of the aforementioned procedures between the other Policies of the Company, the contents of this policy will supersede the other policies.

OBTAINING STAFF ACKNOWLEDGEMENT OF UNDERSTANDING THE REQUIRMENTS OF THIS POLICY DOCUMENT

HOD is required to maintain a log and sign off all staff to ensure this policy document has been read and understood by each staff member coming under HOD's purview.

Staff member(name)……

Head of the Department/(name) ……