PEOPLE'S BANK

POLICY & PROCEDURES

ON

ANTI MONEY LAUNDERING (AML)

AND

COMBATING OF FINANCING OF TERRORISM (CFT)

JANUARY 2023

(VERSION 1.8)

CONTENTS

		Page Nos.
1	People's Bank Policy on Anti Money Laundering and Combating of Financing of Terrorism	05-07
2	Legal Framework for Anti Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) in Sri Lanka	08-10
3	Financial Intelligence Unit Rule No. 01 of 2016- Financial Institutions (Customer Due Diligence) Rules	11-29
4	Applicability of FIU Rule No. 01 of 2016	30-32
5	Suspicious Transaction/ Business	33-38
6	Anti Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) – Monitoring and Controls	39-40
7	Risk Categorization Methodology	41-42
8	Risk Management	43-45
9	Identification of Beneficial Owners	46-47
10	Politically Exposed Persons	48-51
11	Glossary	52-54
12	Attachments: i. Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 1 of 2018 ii. Guidelines for Financial Institutions on Suspicious Transactions Reporting No. 6 of 2018 iii. Guidelines on CCTV operations iv. Guidelines on Identification of beneficial Ownership for Financial Institutions, No. 4 of 2018 v. A list of categories of customers that can be considered as PEPs vi. A list of Red Flags and Indicators for suspicion vii. Guidelines for Non Face to Face Customer Identification and Verification No 3 of 2020	

►*Introduction*

Money Laundering and Terrorist Financing undermine confidence in the International Financial System. The challenges in the fight against Money Laundering and Terrorist Financing are vast, and potential threats exist in every corner of the world. Regulators and Law Enforcement Agencies work hard to stay ahead of increasingly sophisticated criminals seeking to exploit the Global Financial System.

We at People's Bank are committed to the fight against Money Laundering and Terrorist Financing. As a leading Bank in Sri Lanka which has more than 735 Branches and maintaining over 22 Million customer accounts and processing thousands of transactions a day, People's Bank could always be a target for would be money launderers and terrorist financiers.

We believe that no customer relationship is worth compromising our commitment to combating money laundering and terrorist financing. To fulfill this commitment, we have established an independent unit; Compliance Department headed by a Chief Compliance Officer and has taken following steps:

- ✓ Appointed a Chief Compliance Officer who also functions as the Anti Money Laundering Compliance Officer
- ✓ Train employees in Money Laundering and terrorist Financing Prevention practices and controls.
- ✓ Develop systems to capture would be money launderers and terrorist financiers.

Also the intensity and extensiveness of the risk management function of the Bank operates in compliance with the Risk Based Approach and proportionate to the nature, scale and complexity of the activities and money laundering and terrorist financing risk profile of the Bank.

The Bank also takes appropriate steps to identify, assess and manage its money laundering and terrorist financing risks in relation to its customers, countries, geographical areas, products, services, transactions and delivery channels.

The Central Bank of Sri Lanka together with the Financial Intelligence Unit (FIU) have issued directives named Financial Institutions (Customer Due Diligence) Rules requiring Banks to follow certain laid down procedures for opening accounts, maintenance of accounts and monitoring transactions of a suspicious nature.

This Anti Money Laundering (AML) and Combating of Financing of Terrorism (CFT) Policy is prepared based on the said rules issued by the Financial Intelligence Unit of Central Bank of Sri Lanka.

1. PEOPLE'S BANK POLICY ON ANTI MONEY LAUNDERING AND COMBATTING OF FINANCING OF TERRORISM

Banks and Financial Institutions have to take steps to combat the risks of Money Laundering and Terrorist Financing (ML & TF) in order to assist regulators in their fight against ML & TF.

It is the paramount duty and responsibility of the Bank to know and understand its customers fully in terms of identity and activity to the extent of establishing the correctness/genuineness of the credentials for extending better Customer Service.

This exercise also helps the Bank to identify adverse conditions, if any, associated with the applicant/customer (at the time of establishing banking relationship) and guard against criminals/fraudsters making use of banking channels/services for their nefarious activities.

With the present day multifarious dimensions of deliverance of banking services and products, the need for a structured methodology for understanding customers at the time of establishing banking relationship has assumed great importance.

A few steps taken at People's Bank in this regard are

- Establishment of a Compliance Department under the Chief Compliance Officer who is dedicated to the task of overseeing People's Bank's policies, practices and procedures with regard to ML & TF.
- Establishment of a 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 Banks compliance with applicable ML & TF laws, rules and regulations.
- The Bank relies on those closest to its customers - the local Branch Manager to provide guidance and understand fully with whom we are doing business with – "**Know Your Customer" (KYC)** and to ensure that the business we conduct on behalf of our customers is proper.
- Development of internal procedures and technology that assists the Bank in monitoring transactions for the purpose of identifying possible suspicious activities.
- The Bank will continue to update its policies and procedures that meet or exceed applicable norms in the Banking Industry both locally and globally.
- Submitting reports on AML/ CFT risk on a quarterly basis to the Board of Directors to enable the Board to take necessary steps to mitigate the risk.
- The Bank recognizes and is aware that preventing ML & TF and adhering to KYC principles is an on going process that involves constant diligence and the difficulties faced when the Bank tries to keep pace with the ever more sophisticated schemes employed by criminals.

In line with the directives received, a policy document with following sections covering various functional aspects of KYC norms and Anti Money Laundering and Combating of Financing of Terrorism (AML & CFT) measures are set out herein.

a) What is Money Laundering and Terrorist Financing
b) The Sri Lankan Legislation
c) Know Your Customer (KYC) and Customer Due Diligence (CDD), based on the Financial Institutions (Customer Due Diligence) Rule No. 1 of 2016 issued by the Central Bank of Sri Lanka.
d) Applicability of the Directive at People's Bank
e) Identifying and reporting Suspicious Transactions
f) Risk Management and Monitoring Controls
g) Beneficial Owners
h) Politically Exposed Persons

A. What is Money Laundering

Definition of "Money Laundering"
Various Definitions are given to the term "Money Laundering". Set out below are two of the most commonly used ones.

Definition 1. "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 a legitimate source"

Definition 2 "The process by which criminals seek to disguise the illicit nature of their proceeds by introducing them into the stream of legitimate commerce and finance"

B) The Process of Money Laundering
In the process of Money Laundering, there are, theoretically four factors that are common to Money Laundering operations.

a) The real source of criminal money must be concealed and will not be done with public knowledge.

b) The form in which money is held must be changed in order to hide identity.

c) The trail of transaction must be obscured to defeat any attempted follow-up by law enforcement agencies.

d) The launderer must maintain constant control on the monies as he cannot legally declare any theft of such money.

C. Stages of Money Laundering

Money Laundering occurs in three stages -

Stage 1- Placement
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.

D. 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

1. 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:

    a) 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

    b) 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

    c) any terrorist act.

2. 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 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. 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 2006 was amended by Prevention of Money Laundering (Amendment) Act No.40 of 2011. Some of the main features of these three Acts are given below.

A) PREVENTION OF MONEY LAUNDERING ACT (PMLA)

- 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/ Banks) 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.

- In terms of the PMLA Money Laundering is liable to a penalty of not less than the value of the property involved in the offence and not more than thrice this value, and a term of imprisonment of not less than 5 years and not more than 20 years or both to such fine and imprisonment.

- Property derived from an offence of Money Laundering is forfeited to the State free of encumbrances in terms of the PMLA.

- PMLA makes "tipping-off" (pre warning suspects of impending action against them) an offence.

- The extradition law applies to the offence of Money Laundering.

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 indictment of a person for an offence under the Act, all funds collected in contravention of the Act will be frozen (if lying in a bank account) or seized (if held in the control of any person or institution other than a bank).

- 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.

3. 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 banking 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 banking and other types 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 hereunder. These rules are issued under Section 2 of the Financial Transactions Reporting Act No.6 of 2006 and any contravention of, or non-compliance with the same will be liable to the penalties under the relevant provisions of the Act.

A. Provisions on Money Laundering and Terrorist Financing Risk Management Rules

As required by the above rules the Bank 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.

✓ The Bank shall, using the AML system in place verify whether any prospective customer or beneficiary appears on any list of designated persons or entities issued under the regulations made in terms of United Nations Act No.45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism & terrorist financing and proliferation of weapons of mass destruction and its financing or whether such prospective customer or beneficiary acts on behalf of or under the direction of such designated persons or entities or for the benefit of such designated persons or entities .

✓ The risk control and mitigation measures implemented shall be commensurate with the risk level of a particular customer as identified based on risk profiling.

✓ After the initial acceptance of a customer, the Bank shall regularly review and update the risk profile of the customer based on his level of money laundering and terrorist financing risk.

✓ The money laundering and terrorist financing risk management of the Bank shall be affiliated and integrated with the overall risk management of the Bank.

✓ The Bank shall provide a report of its risk assessment, money laundering and terrorist financing risk profile and the effectiveness of its risk control and mitigation measures to the Board of Directors on a monthly basis. This report shall include

- Results of monitoring activities carried out for combating money laundering or terrorist financing risks.
- Details of recent significant risks involved in either internally or externally and its potential impact to the Bank
- Recent developments in written laws on money laundering and suppression of terrorist financing and its implications for the Bank.

CDD for All Customers

➢ The Bank shall not open, operate or maintain any anonymous account, any account in a false name or in the name of a fictitious person or any account that is identified by a number only (hereinafter referred to as numbered accounts)

Numbered accounts include accounts where the ownership is transferrable without the knowledge of the Bank and accounts that are operated and maintained with the account holder's name only.

➢ The Bank shall maintain accounts in such a manner that assets and liabilities of a given customer can be readily retrieved. Accordingly the Bank shall not maintain accounts separately from the usual operational process, systems or procedures of the Bank.

➢ The Bank shall conduct the CDD measures specified in Rule No. 1 of 2016, on customers conducting transactions when

a. Entering into business relationships;

b. Providing money and currency changing business for transactions involving an amount exceeding Rs. 200,000/- or its equivalent in any foreign currency;
c. Providing wire transfer services;
d. Carrying out occasional transactions involving an amount exceeding Rs. 200,000/- or its equivalent in any foreign currency where the transaction is carried out in a single transaction or in multiple transactions that appear to be linked;
e. The Bank has any suspicion that such customer is involved in money laundering or terrorist financing activities, regardless of amount; or
f. The Bank has any doubt about the veracity or adequacy of previously obtained information.

- 1. The Bank shall-
  a. Identify its customers prior to entering into business relationships;
  b. Obtain the information specified in Rule No. 1 of 2016, verify such information, as applicable and record same for the purpose of identifying and initial risk profiling of customers, at the minimum;
  c. Obtain following information for the purpose of conducting CDD, at minimum:
     i. Purpose of the account;
     ii. Sources of earning;
     iii. Expected monthly turnover;
     iv. Expected mode of transactions;
     v. Expected type of counterparties (if applicable).

  2. If any customer is rated as a customer posing a high risk, the Bank shall take enhanced CDD measures for such customer, in addition to the CDD measures stated above.

- If the customer is not a natural person, the Bank shall take reasonable measures to understand the ownership and control structure of the customer and determine the natural persons who ultimately own or control the customer.

- If one or more natural persons are acting on behalf of a customer, the Bank shall identify the natural persons who act on behalf of the customer and verify the identity of such persons. The authority of such person to act on behalf of the customer shall be verified through documentary evidence including specimen signatures of the persons so authorized.

- If there is a beneficial owner, the Bank shall obtain information to identify and take reasonable measures to verify the identity of the beneficial owner of the customer using relevant information or data obtained from a reliable source, adequate for the Bank to satisfy itself that the Bank knows who the beneficial owner is.

- The Bank shall verify the identity of the customer and beneficial owner before or during the course of entering into a business relationship with or conducting a transaction for an occasional customer.

  Provided however, where the risk level of the customer is low as per the risk profile of the Bank and verification is not possible at the point of entering into the business relationship, the Bank may, subject to the below provision, allow its customer and beneficial owner to furnish the relevant documents subsequent to entering into the business relationship and subsequently complete the verification (this shall be called as “delayed verification”)

- In any case where the delayed verification is allowed following conditions shall be satisfied:
  a. Verification shall be completed as soon as it is reasonably practicable but not later than 14 working days from the date of opening the account;

b. The delay shall be essential so as not to interrupt the normal conduct of business of the Bank; and
c. No suspicion of money laundering or terrorist financing risk shall be involved.

- To mitigate the risk of delayed verification, the Bank shall adopt risk management procedures relating to the condition under which the customer may utilize the business relationship prior to verification.

- The Bank shall take the measures to manage the risk of delayed verification which may include limiting the number, type and amount of transactions that can be performed, as stated in chapter 4 of this Policy.

- If the Bank is unable to act in compliance with the above, it shall
  a. In relation to a new customer, not open the account or enter into the business relationship or perform the transaction; or
  b. In relation to an existing customer, terminate the business relationship, with such customer and consider filing a suspicious transaction report in relation to the customer.

- The Bank shall not, under any circumstances, establish a business relationship or conduct any transaction with a customer with high money laundering and terrorist financing risk, prior to verifying the identity of the customer and beneficial owner.

- The Bank shall monitor all business relationships with a customer on an ongoing basis to ensure that the transactions are consistent with the economic profile, risk profile and where appropriate the sources of earning of the customer.

- i. The Bank shall obtain information and examine the background and purpose of all complex, unusually large transactions and all unusual patterns of transactions, which have no apparent economic or prima facie lawful purpose.

  ii. The background and purpose of such transactions shall be inquired into and findings shall be kept in record with a view to making such information available to the relevant competent authority when required and to make suspicious transaction reports.

- The Bank shall report transactions inconsistent with the rules stated in Rule No 1 of 2016 to the Chief Compliance Officer for appropriate action.

- The Bank shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers.

  The review period and procedure shall be decided by the Bank from time to time as appropriate, and shall be decided on a risk based approach.

- The frequency of the ongoing CDD or enhanced ongoing CDD shall commensurate with the level of money laundering and terrorist financing risks posed by the customer based on the risk profiles and nature of transactions.

- The Bank shall increase the number and timing of controls applied and select patterns of transactions that need further examination when conducting enhanced CDD.

- The Bank shall perform such CDD measures as may be appropriate to the existing customers based on its own assessment of materiality and risk but without compromise on the identity and

verification requirements. In assessing the materiality and risk of an existing customer, the Bank may consider the following-

a. The nature and circumstances surrounding the transaction including the significance of transaction;
b. Any material change in the way the account or business relationship is operated; or
c. The insufficiency of information held on the customer or change in the information of the customer.

- The Bank shall conduct CDD on existing customer relationships at appropriate times, taking into account whether and when CDD measures have previously been conducted and the adequacy of data obtained.

- If an existing customer provides unsatisfactory information relating to CDD, the relationship with such customer shall be treated as a relationship posing a high risk and be subjected to enhanced CDD measures.

- If the Bank forms a suspicion of money laundering or terrorist financing risk relating to a customer and it reasonably believes that conducting the process of CDD measures would tip off the customer, the Bank shall terminate conducting the CDD measures and proceed with the transaction and immediately file a suspicion transactions report.

Occasional Customers, One off Customers, Walk in Customers and Third Party Customers

- The Bank 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 walk in 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 Bank has reasonable grounds to suspect that the transaction or series of linked transactions are suspicious or unusual, the Bank shall, obtain such information irrespective of the amount specified above.

CDD for Legal Persons and Legal Arrangements

- The Bank 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 Bank 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 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 Bank shall identify the natural person who controls the legal person.

- In order to identify the beneficial owners of a legal arrangement, the Bank 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.

Non Governmental Organizations, Not for Profit Organizations or Charities

- The bank shall conduct enhanced CDD measures when entering into 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 Bank 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 Bank 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 Bank 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 Bank 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 Bank shall file a Suspicious Transaction Report or take other legal action or take both steps.

Customers and Financial Institutions from High Risk Countries

- 1. The Bank shall apply the enhanced CDD measures to business relationships and transactions to customers and Financial Institutions from high risk countries.

  2. 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-

  i. based on the Financial Action Task Force listing; or

  ii. 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.

  iii. Upon specifying the high risk countries as specified in (ii) above the Bank shall publish the list of high risk countries in its official website.

  iv. The type of enhanced measures applied under (i) above shall be effective and correspond to the nature of risk.

- In addition to enhanced CDD measures, the Bank shall apply appropriate counter measures, as follows, for countries specified in the list of high risk countries referred to in (ii) 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.

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 Banks with a set of instructions on the definition, identification, reviewing and managing the risk associated with PEPs. Accordingly the Bank 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 Bank 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 Deputy General Manager (Channel Management) of the Bank 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 ownership of funds and wealth; and
d. Conduct enhanced ongoing monitoring of business relationships with the politically exposed person.

- The Bank 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.

Correspondence Banks

- When providing correspond banking services to respondent banks the correspondent bank shall take necessary measures to ensure that the risk of money laundering and terrorist financing through the accounts of the respondent banks are duly managed.

  Accordingly, the bank shall assess the suitability of the respondent bank by taking the following measures;

(a) gather adequate information about the respondent bank to thoroughly understand the nature of the respondent bank's business, including the following:-

(i) internal policy of the respondent bank on anti-money laundering and suppression of terrorist financing;

(ii) information about the respondent bank's management and ownership;

(iii) core business activities;

(iv) Country of geographical presence, jurisdiction or country of correspondence;

(v) Money laundering prevention and detection measures;

(vi) The purpose of the account or service;

(vii) Identity of any third party that will use the correspondent banking services (*i.e.* in case of payable through account);

(viii) The level of the regulation and supervision of banks in the country of the respondent bank.

(b) Determine from publicly available sources, the reputation of the respondent bank, and as far as practicable, the quality of supervision over the respondent bank, including facts as to whether it has been subject to money laundering or terrorist financing or regulatory action;

(c) Assess the respondent bank's anti-money laundering and suppression of terrorist financing systems and ascertain whether they are adequate and effective, having regard to the anti-money laundering and suppression of terrorism financing measures of the country or jurisdiction in which the respondent bank operates;

(d) Clearly understand and record the respective anti-money laundering and suppression of terrorist financing responsibilities of each bank; and

(e) Obtain approval of the Board of Directors or a Committee appointed by the Board of Directors of the respondent bank, before entering into new correspondent banking relationships.

- The bank shall in relation to "payable-through accounts", satisfy itself that the respondent bank-

(a) Has conducted CDD measures on its customers that have direct access to the accounts of the correspondent bank; and

(b) Is able to provide relevant CDD information upon request to the correspondent bank.

- The bank shall apply enhanced CDD measures when entering into or continuing correspondent banking relationship with banks or Financial Institutions which are located in high risk countries.

- The bank shall not enter into or continue correspondent banking relationship with a shell bank.

When providing correspondent banking services, the bank shall take appropriate measures to satisfy itself that its respondent Financial Institutions do not permit their accounts to be used by shell banks.

Wire Transfers

- The Bank 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 Bank 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 Bank 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 Bank 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 Bank 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 Bank 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 Bank shall make the information available as soon as practicable after receiving the request either from the Beneficiary Financial Institution or from the appropriate authority.

- The Bank 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 Bank 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.

Intermediary Financial Institution

- The Bank when involved in wire transfers as an Intermediary Financial Institution shall ensure that for cross-border wire transfers, all originator and beneficiary information that accompanies a wire transfer is retained with the wire transfer message.

- Where technical limitations prevent the required originator or beneficiary information accompanying a cross- border wire transfer from remaining with a related domestic wire transfer, the Bank shall keep a record, for at least twelve years, of all the information received from the ordering Financial Institution or another Intermediary Financial Institution.

- The Bank shall take reasonable measures, which are consistent with straight- through processing to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

- The Bank shall have risk-based internal policies and procedures for determining-

  (a) when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and

  (b) what is the appropriate follow up action.

Beneficiary Financial Institution

- The Bank shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

- For cross-border wire transfers, the Bank shall verify the identity of the beneficiary, and maintain the information in accordance with the Act if the identity has not been previously verified.

- The Bank shall have risk-based internal policies and procedures for determining-

  (a) when to execute, reject or suspend a wire transfer with insufficient, originator or beneficiary information; and

  (b) what is the appropriate follow up action

Money or Value Transfer Service Providers

- When conducting Money or Value Transfer Service (hereinafter referred to as "MVTS") the Bank shall maintain a current list of its agents in all countries in which the MVTS provider and its agents operate.

- The Bank if agents are used shall include them in its internal policy on Anti-money Laundering or Suppression of Terrorist Financing and monitor them in compliance with that policy.

- At instances where any amendments take place in the list of Agents those amendments will be circulated through Internal Circulars.

- The Bank shall comply with the provisions applicable for CDD in wire transfers, when operating directly or through their agents in Sri Lanka, or shall comply with similar requirements issued by a relevant authority, when operating directly or through its agents in a foreign country.

- When the Bank controls the ordering customer as well as the beneficiary customer of a wire transfer, shall –

  (a) take into account all relevant information from the ordering customer and the beneficiary customer, in order to determine whether a suspicious transaction report needs to be filed; and

  (b) file a suspicious transaction report with the Financial Intelligence Unit, on identifying a suspicious wire transfer.

- 1. The Bank shall follow special precautionary measures to make a distinction between formal money transmission services and other alternative money or value transfer systems (ex: hundi, hawala etc.) through which funds or value are moved from one geographic location to another, through informal and unsupervised networks or mechanisms.

1. The Bank shall take reasonable measures to ascertain the sources of funds involving any such alternative money or value transfer system and file a suspicious transaction report with the Financial Intelligence Unit.

B. Account Opening Guidance

I. Face to Face

1. Individual Customer

(a) The following information shall be obtained:

(a1) 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

(a2) 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 instructions

(b) 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.

The examples quoted above are not the only possibilities. In particular jurisdictions there may be other documents of an equivalent nature which may be produced as satisfactory evidence of customers' identity.

The Bank should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview.

II. Non Face to Face

In pursuant with section 15(1) of the Financial Transactions Reporting Act No. 6 of 2006, the Financial Intelligence Unit of Central Bank of Sri Lanka has issued Guideline No. 3 of 2020 on Non Face to Face Customer Identification and Verification. In compliance with these Guidelines which have to be read with Financial Transactions Reporting Act No. 6 of 2006 and Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 which are detailed above, the Bank has adopted following process to open accounts of non face to face customers.

1. The Bank shall act in compliance with the requirements stated in Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 and shall follow the alternate methods introduced by Guideline No. 3 of 2020 to verify the identity document and the address.
2. The Bank shall follow safe and trustworthy methods to obtain identification information such as
    - electronic forms,
    - mobile app,
    - video conferencing,
    - secure email,
    - kiosks (ATMs, CDMs),
    - registered post etc.

    and shall not use agents, third party service providers acting as agents, third party financial institutions, designated non finance businesses to collect identification information. Also steps shall be taken by the Bank to obtain high quality still images of the customer, ID documents and address verification documents.
3. Also steps shall be taken to obtain the quality images of passport
4. The electronic interface provided by Department of Registration of Persons shall be used by the Bank to independently verify the identity of the customer.
5. The Bank shall be responsible with ensuring AML/CFT compliance of all parties involved with online payment platforms introduced by the Bank and shall take steps to act in compliance with the provisions of Financial Transaction Reporting Act, Financial Institutions (Customer Due Diligence) Rules and all other Rules, Regulations and Guidelines issued thereunder in relation to followings for all parties involved in online payment platforms.
    - Identification and verification of customers
    - Conduct ongoing due diligence on customers and scrutiny of transactions
    - Identification and reporting of suspicious transactions
    - Wire transfer requirements
    - Targeted financial sanctions screening
    - Record keeping
    - All other reporting requirements

C. General Provisions

1. The Bank is required to appoint a Key Management Person who is from Senior Management level of the Bank as the Chief 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 Chief Compliance Officer or any other person 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 including 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.

5. Maintain an independent audit function in compliance 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 Bank 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.

7. The Bank shall 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.

8. The Bank shall
   - ✓ Undertake the risk assessments prior to the launch or use of new products 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 and
   - ✓ Monitor pre-loading of credit cards, as that may amount, inter-alia, to the abuse of credit cards, for money laundering or terrorist financing purposes, file a Suspicious Transaction Report if suspicious transactions are detected.

D. <u>Record Keeping</u>

9. The Bank shall maintain all records of transactions, both domestic and international, including the results of any analysis undertaken, such as inquiries to establish the background and purpose of complex, unusually large transactions for a minimum period of twelve years from completion of such transaction.

10. The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transactions, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to be produced in a Court of Law, when necessary, as evidence. The transaction records may be maintained in document form, by electronic means, on microfilm or in any other form that may be admissible as evidence in a Court of Law.

11. The records of identification data obtained through CDD process such as copies of identification documents, account opening forms, know your customer related documents, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of twelve years commencing from the date on which the business relationship was fulfilled or the occasional transaction was effected.

12. The records shall be maintained up to date and be kept in original or copies with the attestation of the Bank.

13. The Bank shall retain the above records for a longer period if transactions, customers or accounts are involved in litigation or required to be produced in Court of Law or before any other appropriate authority.

14. The Bank shall ensure that all CDD information and transaction records are available immediately to relevant domestic authority and Financial Intelligence Unit.

For the purpose of this rule relevant domestic authority means-

a. Any public authority (including a supervisory authority established as independent non-governmental authority with statutory powers) with designated responsibilities for prevention of money laundering and suppression of terrorist financing;
b. Any authority that performs the function of investigating and prosecuting money laundering and terrorist financing associated offences and seizing or freezing and confiscating assets relating to such offences; and
c. Any authority receiving reports on cross border transportation of currency.

15. The Bank shall train the staff on all issues related to AML/CFT. The training shall be provided for all staff upon joining and after that once in every two years. Apart from general training provided to all staff, targeted training programs shall be conducted for specific categories of staff. Also AML/ CFT training shall be conducted for members of Board of Directors.

E. Miscellaneous

16. In the case of a prospective customer whose permanent address given in the application is at a location far away from that of the branch which receives the account opening request, the Bank shall discourage or turn down the request to open the account and shall request the prospective customer to open the account at the closest branch to the residence or business of the customer, unless an acceptable and a valid reason is given to keep in record.

17. Where two or more accounts are opened in the Bank by one customer, the Bank shall record the specific purpose for which such accounts are opened, in order to enable ongoing CDD of all accounts.

18. Unless and until adequate identity of the prospective client is obtained no account shall be opened. If any discrepancy in information is detected subsequently the account shall be suspended until the veracity of such information is confirmed.

19. Copies of all identification and address verification documents shall be retained in terms of the law.

20. When instructions are received from clients to transfer funds from one account to another both account numbers shall be recorded internally to aid future reference.

21. When Foreign Currency Accounts and temporary rupee accounts are opened for non-nationals/foreign passport holders who are resident in Sri Lanka, a local address shall be obtained as their permanent address during their stay in the Island. A copy of the passport, visa with validity period, foreign address and the purpose for which the account is opened shall be made available in the file. On the expiry of the visa, the account shall cease to operate unless and otherwise appropriate instructions are received. On leaving the Island the account shall either be closed or be converted into a non-resident account. The Bank shall ensure that a valid visa is held at all times by the clients during the continuation of the account with them.

22. When Rupee Accounts are opened and maintained for non-residents (foreign passport holders), the foreign address shall be used as the permanent address and for all correspondence. The reason for choosing to open the account in a foreign jurisdiction shall be recorded in the file.

23. All cash deposits made into savings and current accounts over Rs.200,000/= by third parties shall have on record, the identity of the depositor. The required details are, the name, address, Identification number of a valid identification document, purpose and the signature. However, clerks, accountants and employees of business houses who are authorized to deal with the accounts shall not be treated as “third parties”.

24. The Bank shall ensure that no Automatic Teller Machine (ATM) withdrawals exceeding the mandatory threshold are made without the expressed approval of the Bank. If regular withdrawals are made by customers in small amounts in order to circumvent the reporting limit, they shall be reported as a suspicious transaction. The Bank shall exercise due diligence to prevent any misuse of this facility. This is applicable to both rupee accounts and foreign currency accounts.

25. Accounts which record frequent transactions below the threshold limit of Rs.1,000,000/= in an attempt to circumvent the mandatory reporting requirement, shall be reported to the Chief Compliance Officer for appropriate action.

26. The Bank will ensure that account activities are consistent with the customer profile on record. Any inconsistency shall be inquired into and the correct position recorded. All unexplainable activities shall be reported to the Chief Compliance Officer for appropriate action.

27. When applications for opening of accounts are received by mail or e-mail due care should be exercised to record the true identity of the client prior to opening the accounts or activating them. In no case shall the Bank short-circuit the required identity procedures just because the prospective client is unable to present himself in person.

The Guideline No.1 of 2018 issued by Financial Intelligence Unit on Money Laundering & Terrorist Financing Risk Management for Financial Institutions is attached.

4. APPLICABILITY OF FIU RULE NO. 01 OF 2016

This section of the Policy is to ensure that People's Bank has internally developed effective Anti Money Laundering and Combating of Financing of Terrorism procedures to reduce the risk of the Bank 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 Bank 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 Bank being unwittingly involved in the activities of third parties, who may seek to use bank facilities to hide the source of criminal funds.

As such,

- ✓ The Bank 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 correspondent banking services, 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, Regional 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.

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 Operations Manager/ 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 Operations Manager/ 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 Bank-

- 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 Bank.

d) The Operations Manager/ 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.

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 Chief 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 Regional Managers, 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. An e-learning module has been included in the Intranet of the People's Bank and all Department Heads and Branch Managers shall ensure that all operational and Front Office staff has gone through same and are familiar with the provisions therein.

3. A Certificate on Compliance with the procedures contained in this Policy; would need to be submitted by the Branch Managers to the Chief 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/ Operations 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 Regional Compliance Officer. A summary of such accounts opened with current status should be submitted to the Regional Compliance Officer on a monthly basis. The Regional Compliance Officer should collate these and submit a Quarterly Report to the Chief 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.

   e) In the event the KYC cannot be successfully completed in 3 months, the account should be closed and the funds returned to the source from which they were received in the same manner the deposit was made.

iii) It shall be the duty of the In-House Auditor of each Branch to check on the status of documentation for all new accounts opened on a daily basis and enter variances and exceptions in a Register to be maintained for this purpose. This will be subjected to audit by the Internal Audit Department and the Compliance Department of the Bank.

5. 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 Bank has to establish and maintain procedures and systems to implement the reporting requirement under Section 7 of the FTRA. Further, Section 14 (1) (d) requires the Bank to train its officers employees and agents to recognize suspicious transactions.

The Bank has put up an AML system with rules/ scenarios to identify suspicious transactions. All alerts generated by the system shall be evaluated by the Compliance Department and if necessary forwarded to the branches for their feedback. The branches shall send their feedback to Compliance Department and the Compliance Department shall file the Suspicious Transaction report accordingly.

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.

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 transactions is to know enough about the customer to recognize that a transaction, or series of transactions, is unusual for that particular customer. While the following provide some examples, recognizing suspicious transactions is a matter of good sense and attention to detail.

Suspicious Cash Transactions

1. Unusually large cash deposits made by an individual or a company whose normal business activities would mainly be conducted by cheques or other instruments.

2. Substantial increase in cash deposits by any customer or the Bank 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.

3. 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.

4. 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.

5. Customers who constantly pay-in or deposit cash to cover requests for Bankers drafts, money transfers or other negotiable instruments without an apparent reason.

6. Customers who seek to change large quantities of lower denomination bank notes for those of higher denomination banknotes with no obvious reasons.

7. Customers who transfer large sums of money outside the country with instructions for payment in cash, and large sums transferred from outside the country in favour of non-resident customers with instructions for payment in cash.

8. Unusually large cash deposits using "ATMs" or "Cash Deposit Machines" to avoid direct contact with the employees of the relevant license, if such deposits are not consistent with the business/normal income of the concerned customers.

Suspicious Transactions using Customers' Accounts

1. 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.

2. Customers who have numerous 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 banking relationships with banks which extend them facilities from time to time.

3. Any individual or company whose account shows virtually no normal personal banking or business-related activates, 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 (e.g. substantial turn-over in the account).

4. Customers who have accounts with several Banks within the same locality and who transfer the balances of those accounts to one account, then transfer the consolidated amount to a person abroad.

5. Paying-in large third party cheques endorsed in favour of the account holder when they do not seem to be relevant to the account holder and his nature of business.

6. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received unexpected large sums of money from abroad.

7. A large number of individuals who deposit monies into the same account without an adequate explanation.

8. Unusually large deposits in the accounts of a jewellery shop whose accounts have never witnessed such deposits particularly, if a large part of these deposits is in cash.

Suspicious Investment Related Transactions:

1. Purchasing of securities to be held by the Bank in safe custody, where this does not appear appropriate given the customer's apparent standing. (Financial income etc.)

2. Individual or commercial institutions which bring in large sums of money to invest in foreign currencies or securities, where the size of transactions are not consistent with the income of the concerned individual or commercial institutions.

3. Buying or selling securities with no justifiable purpose or in circumstances, which appear unusual.

Suspicious Transactions using Electronic Banking Services

1. When an account receives numerous small fund transfers electronically, and then the account holder carries out large transfers in the same way to another country.

2. Where a customer makes regular and large payments using different means including, electronic payments that cannot be clearly identified as bona-fide transactions, or receive regular and large payments from countries known for serious criminal activities.

3. Where transfers from abroad, received in the name of a customer of the bank or any financial institution electronically are transferred abroad in the same way without passing through an account (i.e. they are not deposited then withdrawn from the account). Such transactions should be registered in the account and should appear in the account statement.

Suspicious International Banking and Financial Transactions

1. Customers introduced by a branch outside the country, and affiliate or another bank, based in one of the countries known for the production or consumption of drugs or other serious criminal activities.

2. Building up of large balances not consistent with the known turnover of the customer's business and the subsequent transfer to account(s) held abroad.

3. Frequent requests for foreign currency drafts or other negotiable instruments, for no obvious reasons.

4. Frequent paying-in of foreign currency drafts in large amounts for no obvious reasons, particularly if originating from abroad.

Suspicious use of Letters of Credit (LC)

1. Where the applicant of LC (customer of bank) and the beneficiary of LC are same individuals/ entities.

2. Where the Bank's customer who opens these letters is the beneficiary and the owner of the shipping company.

3. Where amounts on letters of credit submitted by the customer to the bank and to the Customs/Ports/Airport authorities do not match the original.

4. Where the size of the facilities are not in line with the securities on hand, nature of business and net-worth of the customers.

5. Where such trade is not consistent with the customer's usual business.

Suspicious Loan Transactions:

1. Customers who repay classified/problem loans before the expected time and in larger amounts than anticipated.

2. 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.

3. Non-resident individuals who request loans secured by bank guarantees issued by foreign banks where the purpose of the transaction is questionable.

4. Loan transactions against pledge of deposits with financial institutions outside the country, especially if these were in countries known for the production, processing or consumption of drugs or other criminal activities.

Informal Value Transfer Systems (IMVTS)

1. Receipt of foreign remittances to accounts initially and its gradual decrease/cessation followed by the receipt of Sri Lankan Rupees.

2. Receipt of frequent third-party deposits and transfer of those funds to multiple third party accounts.

3. Minimal / no ATM withdrawals but substantial number of online debit fund transfers from accounts with names of receivers as narrations.

4. Receipt of frequent third-party deposits and withdrawal of such funds from abroad.

5. Accounts having an insignificant daily balance but an unusually high credit and debit turnover.

6. It inquiries are made by the Bank, accountholders themselves declaring to be engaged in IMVTS operations.

Scams

1. A local person establishes a banking relationship on behalf of a third party, maybe a foreigner.
2. The accounts are operated by a third party or a foreigner(s).
3. Often customers' use of forged / stolen NICs to establish business relationships.
4. The customer's company name is very similar to a very well-known, global company name, but not quite the same (e.g., P&G Printing, GE Electricians, Amazing Books)
5. The customer's company name or email address is not available in the internet.
6. The individual who operates the account(s) hardly visits a bank branch.
7. Majority of ATM transactions are carried out from locations which are not in the vicinity of the customer's residential address or the employment address.
8. The withdrawals are carried out using ATM machines and often they use the ATMs of the other banks.
9. Often uses ATMs situated in under-lit areas.
10. Avoids the CCTV cameras at or in the vicinity of ATMs.
11. The account holder cannot be contacted: the correspondence sent to the customer repeatedly returned as undeliverable despite having an active account with ongoing transactions.
12. Deposits are made stating the purpose as "custom fees", "clearance fees", etc.
13. Frequent third-party deposits but depositors identify themselves in the deposit slip or in the remarks in an online transfer using their names and NICs.
14. An inquiry or a complaint from a third party regarding the account stating that the account holder is collecting funds.

Recognizing & Reporting Of Suspicious Transactions

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

Reporting
In the first event of your suspicion:

- The staff concerned should report the same immediately to the immediate superior to ensure that there are no known facts which would negate the suspicion.

How to report a Suspicious Transaction

To reiterate, the law requires employees to report any reasonable suspicion that they may have about a customer or his/her transactions.

The law also requires the Bank to have appropriate effective reporting procedures and systems in place to implement the reporting requirement. It also requires that all employees follow these procedures using them correctly as they are intended to be used.

Reporting procedures

Good reporting procedures and their correct use are designed to ensure that, when a suspicious transaction has been identified -

- the suspected customer or any other related person is not alerted
- the matter is dealt with quickly and professionally
- the external authorities are notified and provided with the necessary records, if appropriate

The Bank has put in place procedures to report suspicions with supporting information,

i. Through the format issued to the branch network.
ii. Through the AML system put in place to monitor suspicious activities.

Awareness has been made among the employees to ensure that the supporting information sent is relevant to the suspicion so that it is passed on to the Financial Intelligence Unit (FIU).

Role of the Chief Compliance Officer on receiving the Report

At the Bank,

- when the Chief Compliance Officer receives the Suspicious Transaction Report, (STR) the Chief Compliance Officer shall decide whether the report gives rise to knowledge or suspicion that a customer is involved in money laundering.
- If further information is needed the Chief Compliance Officer shall collect the required information from the relevant branch/ unit.
- If the Chief Compliance Officer believes that the suspicions may be justified and require further investigation, must report to the Financial Intelligence Unit (FIU)

The Bank may make further enquiries within the parameters of its own records but it does not need to carry out the more detailed criminal investigations.

The employee has a duty to assist the Chief Compliance Officer in reporting the complaint to the FIU effectively, by making sure that the information provided –

- describes why there are reasonable grounds for suspicion and what they are
- contains accurate information
- is timely and not delayed

The importance of timing

The Bank is aware that,

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

- The consequences of not reporting suspicions immediately to the Chief Compliance Officer could be serious for the employee involved and may include individual fines, imprisonment, or both as set out in the legislation.

- 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.

- The above does not mean that the Bank cannot ask the customer for an explanation, or continue to provide them with a normal customer service. But it does mean that the Bank must do so without alerting them to the fact that the Bank may or had already notified the Authorities. If customers being investigated are alerted, the Bank could be blamed for tipping them off, which is a criminal offence for the individual who alerted the customer to the existence of an actual or potential investigation.

- As required by Law, suspicious transactions should be submitted to Financial Intelligence Unit (FIU) as soon as practicably possible but no later than two working days of formation of suspicion.

The Guideline No.06 of 2018 issued by Financial Intelligence Unit on Suspicious Transactions Reporting is attached.

6. ANTI MONEY LAUNDERING (AML) – COMBATING OF FINANCING OF TERRORISM (CFT) MONITORING AND CONTROLS

CHIEF COMPLIANCE OFFICER

Bank has designated the responsibility to control and monitor AML and CFT issues within the Bank to an independent staff designated as "Chief Compliance Officer" with reporting line directly to the Board Integrated Risk Management Committee.

Responsibilities of the Chief Compliance Officer

- Implement Anti Money Laundering and Combating of Financing of Terrorism Policy of the Bank in line with the requirements and update AML & CFT Policy on an ongoing basis in line with local and international requirements.

- Train staff and create awareness on Anti Money Laundering and Combating of Financing of Terrorism requirements.

- Ensure that all departments/ branches conduct their business in accordance with the spirit of the AML & CFT Policy.

- Monitor the day-to-day operations to detect unusual customer activity (as mentioned above under section 'recognising suspicious transactions/business')

- Put in place, policies, procedures and systems to ensure that the Bank will not be used by the money launderers or terrorist financiers.

- Serve as a contact point in the bank for compliance issues:

  a) Provide feedback to staff on compliance queries.

b) Receive internal suspicious transactions report from staff, analyse and investigate the same and liaise with the Financial Intelligence Unit.

c) Take reasonable steps to acquire relevant information from customer or other sources.

d) Report all suspicious money laundering and terrorist financing transactions to Financial Intelligence Unit (FIU)

Independent Compliance Testing

Bank has entrusted Regional Compliance Officers with the responsibility to test the implementation and adherence of the AML & CFT Policy of the Bank. The findings/recommendations should be reported directly to the Chief Compliance Officer. In addition the Compliance Department also carries out random assessments and reviews to verify among other things the implementation and adherence of the AML & CFT Policy in the Bank and report any non-compliances to the Board Integrated Risk Management Committee.

Record Keeping Obligations

In addition to regular bank record keeping requirements, the Anti Money Laundering and Combating of Financing of Terrorism Policy of the Bank requires that documents concerning customer identification and records relating to transactions undertaken on behalf of customers/non customers (all transactions including cash, wire transfers, purchases/sale of monetary instrument etc) be maintained as follows:

- In the case of records that were in existence on 4.8.2016- for a period of not less than ten years from that date.
- In the case of new records created after 4.8.2016- for a period of not less than twelve years from the date of creating the record.

It is also required that :

a) All anti-money laundering and combating of terrorist financing monitoring reports made by Chief Compliance Officer and records of consideration on those reports and of any action taken consequently including reporting done to management/auditors/regulators be maintained as stated above for future reviews.

b) Records showing the dates of anti-money laundering and combating of terrorist financing training and the names and acknowledgement of the staff receiving the training be also maintained as stated above.

All records maintained should be available to authorized persons promptly on request without undue delays.

7. RISK CATEGORIZATION METHODOLOGY

From the information provided by the customer the Bank should be able to make an initial assessment of a customer's risk profile and accordingly special attention needs to be focused on those customers identified thereby as having a higher risk profile. Enhanced Due Diligence (EDD) must be paid on those customer and in order to carry out EDD additional inquiries should be made and information should be obtained in respect of those customers including the following:-

- evidence of an individual's permanent address sought through independent verification by field visits;
- personal reference (i.e. by an existing customer of the same institution);
- prior bank reference regarding the customer and the customer contact with the Bank;
- The customer's source of wealth;
- Verification of details relating to employment, public position held (previous/present), if any, supplied by the customer.
- Obtaining & verifying additional information on the customer such as details of occupation, volume of assets, information available in public data- bases, internet search, etc.)
- Regular updation of identification data of customer and Beneficiary owner
- Obtaining additional information on nature of business
- Obtaining information on reasons for transactions performed
- Obtaining information on source of funds/ wealth of the customer
- Obtaining the approval of Senior Management.

A. Low Risk

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

Example:

Student/Housewife/Pensioner
Employee Non executive –Government
Employee – Non executive -Private
Public Limited Liability Company
Business – Individual
Club/Society/Association
Educational Institution
Self Employed - Professional
Self Employed - Business
Other Individuals

B. Medium Risk

Individuals and entities whose accounts reflect a large volume of turnover or a large number of high value transactions in the estimation of a branch, taking into account the relevant factors such as the nature of business, source of funds, profile, market reports etc. shall be categorised under Medium Risk.

In these cases upon seeking clarification satisfactory responses shall be forthcoming from the customers.

Example:

Employee-Executive-Government
Lawyer & Accountant
Government Institution
Private Limited Liability Company
Business-Proprietor/Partnership

C. High Risk

Individuals and entities whose public image profile in terms of the KYC and AML in the estimation of the Bank is poor/adverse shall be categorised as high risk.

Examples:

PEPs
NGOs
Off Shore/Non Resident Company
Foreign Citizen
Share & Stock Brokers
Investing/Administering/managing public funds
Restaurant/Bar/Casino/Gambling House/Night Club
Importer/Dealers in 2nd hand motor vehicles

Based on the above a KYC Risk categorization Form has been prepared and this document is required to be filled by the Operations Manager/Branch Manager for all accounts opened and attached to the Account Opening Form.

Under normal circumstances the risk status of customers, shall be evaluated and updated based on the risk status as follows;

a. Low Risk Customers – Once in every three years

b. Medium Risk Customers – Once in every two years
c. High Risk Customers – Annually

But at instances where the status of the customer changes, the Bank shall take steps to evaluate and change the customer risk rate accordingly.

8. RISK MANAGEMENT

- This Policy document shall be the benchmark for the supervision of systems and procedures, controls, training and other related matters in the implementation of AML & CFT guidelines in the Bank.

- By the very nature of its functioning, banks are more susceptible to the risk of Money Laundering & Terrorist Financing and the possibility of its various services being unwittingly used for conducting and cycling the ill-effects of the tainted/illegal money by the financial launderers. In this context it is imperative that banks should know its customers, particularly their identity preferably at the time of establishing banking relationship since the incidence or risk factor begins at this point of time-itself.

- The front office functionaries (Counter Staff) at the operational points are vested with greater responsibility of effectively administering KYC procedures to protect bank against financial frauds and Money Laundering & Terrorist Financing. The bank resolves that the KYC requirements shall be realised without inconveniencing the customer and rather it shall be through convincing them that it is well intended in their long term interest and in the interest of the Banking Community and the Regulator.

  Identifying/handling the transactions which are of a suspicious nature, and the procedure that has to be followed when the KYC cannot be completed, have been defined and set out in the previous chapters.

  The operational staff shall continue to be trained on an on-going basis on the basic requirement of proper,
  - Customer identification or KYC
  - Maintenance of records of transactions and identification

- Listing and submission of details of large value currency transactions reports which will certainly help banks to check/reduce operational risks and also vulnerability to frauds.

- The bank shall administer Anti Money Laundering & Combating of Financing of Terrorism measure keeping in view the risk involved in a transaction, account or business relationship for the existing and new customers.

- The bank shall continue to ensure that compliance to KYC guidelines is evaluated periodically in the background of the conditions obtained in respect of the bank's Policies, system and Procedures, Legal and Regulatory requirements. Compliance Report on the implementation of KYC guidelines shall continue to be placed at the Board of Directors monthly.

- The Bank shall ensure that the Internal Audit Department regularly/periodically and the Compliance Department randomly observe audit requirements of KYC guidelines and verification of its implementation at branches and other operational units of the Bank.

CCTV Operations

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

- The Bank 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 Bank shall ensure that the CCTV system is not interfered by internal or external lighting, glare or any other object.

- Bank 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 Bank.

- 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 Bank is closed for business.

- Real time monitoring shall be conducted by the Bank 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 Bank shall maintain information captured in the CCTV system for a minimum period of 90 days but shall retain for a longer period if suspicious activities are observed. Furthermore if instructions are received from Law Enforcement Authorities or any other Competent Authority the Bank shall retain CCTV recordings relevant to a suspicious Transactions Report furnished to FIU until the relevant investigations are concluded.

- The Bank shall ensure that CCTV system is capable of transferring the information to data storage devices.

- The Bank shall,

- Allocate adequate resources with sufficient training
- Ensure that CCTV systems are properly maintained and equipped with relevant features and functions to enable implementing control measures
- Ensure that all information and records are maintained safely and securely without unauthorized access
- Have procedures and mechanisms to ensure that Regulator, Law Enforcement Authorities and FIU are able to obtain information and records
- Put in place periodical review and audit of CCTV systems and submit the report on the same to the Board of Directors and Senior Management
- Ensure that based on the report submitted the Board of Directors and Senior Management shall take appropriate steps to rectify deficiencies identified, increase the coverage, replace or upgrade the equipment
- Ensure activities relating to maintenance and recalibration of CCTV system are clearly recorded in the system's maintenance log and reported to the Senior Management.

Instructions issued by Financial Intelligence Unit are attached.

Training to Staff members (KYC/ AML/ CFT)

- The bank shall ensure that the training sessions on KYC guidelines and AML & CFT procedures are included in the Training Calendar on an ongoing basis. The Bank 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 bank's focussed endeavour to make all those concerned fully understand the rationale behind the KYC/AML & CFT procedures and implement them consistently.

- The Bank'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.

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 bank shall publish this Policy in the Bank'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 present adverse 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 Bank shall endeavour to guard against denial of banking 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.

9. IDENTIFICATION OF BENEFICIAL OWNERS

The Bank shall take steps to determine the ultimate beneficial owners of legal persons and legal arrangements and when a natural person is identified, he should be treated as the beneficial owner unless there are reasonable grounds to show that he is acting on behalf of another person or if another person is the beneficial owner of the property of the customer.

1. The Bank shall take steps to identify the beneficial owner of a legal person considering three main facts stated below and it shall not be necessary to fulfill all three factors to be a beneficial owner.

    - Who are the natural person/s who own or control more than 10% of the customer's equity?
    - Who are the natural person/s who has effective control of the Legal Person?
    - On behalf of which natural person/s is the transaction being conducted?

2. At instances where the ownership is divided among large number of individuals and the shareholding percentage of every individual is less than 10%, the Bank shall take steps to verify the status of Beneficial Ownership by verifying the person/s who hold the Effective Control of the Legal Person or Legal Entity or verifying the person on whose behalf a transaction is being conducted.

3. The Bank shall take steps to obtain and verify information on Trusts including the identities of the author of the Trust, the trustees the beneficiary or class of beneficiary and any other natural person, exercising ultimate effective control over the Trust.

4. Bank shall obtain documents pertaining to Trust (Deed of Trust, Instrument of Trust, Trust Declaration, etc.) and shall verify the provisions provided in the documents within the context of the laws through independent means.

5. The Bank shall take all reasonable measures to verify the identity of the beneficial owner/s using information obtained from reliable sources in order to obtain sufficient information to confirm who the beneficial owner/s is.

6. The identification that shall be obtained are as follows;
    - full name
    - official personal identification or any other identification number
    - permanent/ residential address

7. The Bank shall verify the identity of the beneficial owner before or during the course of entering into a business relationship with, or conducting a transaction for an occasional customer.

8. Furthermore, the Bank shall take steps to identify the beneficial owners through following means;
    - Share Register
    - Annual Returns
    - Trust Deed
    - Partnership Agreement
    - Constitution and/ or Certificate of Incorporation
    - Constitution of a registered co-operative society
    - Minutes of the board meetings
    - Information that can be obtained by open source search or commercially available databases.
    - Verification through mother company or branches, Correspondence Bank, other agents of the Bank, Corporate Registries etc. (for foreign legal persons & arrangements)
    - Relevant identification information available from reliable sources such as public registers (for Companies listed in Stock Exchange)

9. At instances where a beneficial owner is not available & individual person existing control over the customer is not available, the Bank shall identify natural persons holding senior management positions as beneficial owners.

10. The Bank shall review the adequacy of information in respect of beneficial owners according to the risk status of the customer, through obtaining information from the existing core-banking system of the Bank.

11. In addition the review of beneficial ownership shall take place if any material/ significant change as stated below takes place in the customer;
    - A public company is taken private
    - A shareholder or a group of shareholders takes effective control of voting shares
    - A new partner is added or an existing partner is removed
    - Change in management positions
    - New trustees are appointed
    - A Trust is dissolved
    - A new account is opened for the same customer
    - Transactions are attempted that are inconsistent with customer profile

12. A delayed verification is permitted to be carried out to verify the identity of beneficial owners when;
    - risk level of the customer is low & verification is not possible at the point of entering into the business relationship
    - there is no suspicion of money laundering or terrorist financing risk involved
    - delay will not interrupt the normal conduct of business

13. When delayed verification is allowed the Bank should carry out risk management procedures such as, limiting the number, put in restrictions on types and/ or amounts of transactions, monitoring large or complex transactions etc.

14. The Bank shall not establish a business relationship or conduct any transaction with a customer who poses a high money laundering and terrorist financing risk prior to verifying the identity of the beneficial owner.

15. The Bank shall not conduct any business relationship with any customer who is not able to comply with the above provisions.

16. The Bank shall maintain records of identification and verification relating to beneficial ownership for a period of twelve (12) years as stated above.

17. The Bank shall identify if the beneficial owner is a Politically Exposed Person (PEP) & will consider such relationships as high risk and conduct enhanced due diligence.

Guidelines on Identification of Beneficial Ownership for Financial Institutions, No. 04 of 2018 are attached.

10. POLITICALLY EXPOSED PERSONS

Regulatory Framework

The Regulatory framework consist of two regulations issued by the Financial Intelligence Unit (FIU) of Central Bank of Sri Lanka and Financial Action task Force (FATF) recommendations titled International Standards on combating Money laundering and the Finance of Terrorism and Proliferation. Two related regulations issued by FIU are

- Customer Due Diligence Rules No. 01 of 2016
- Guidelines on identification of Politically Exposed persons No. 03 of 2019

Regulatory Definition

An individual who is entrusted with prominent public function either domestically or by a foreign country, or in an international organization and includes

i. A Head of a State or a Government
ii. A Politician
iii. A Senior Government Officer, Judicial Officer or Military Officer
iv. A Senior Executive of a State Owned Corporation/ Government or Autonomous Body
v. Family members and close associates of the above stated PEPs.

Regulatory Descriptions of PEPs

a. **Domestic PEPs:** Individuals who are entrusted with prominent public functions in Sri Lanka.

b. **Foreign PEPs:** Individuals who are entrusted with prominent public functions by a foreign country.

c. **International Organization PEPs:** Persons who are entrusted with a prominent function by an international organization.

d. **Immediate Family Members:** Individuals who are related to a PEP either directly or through marriage or similar forms of partnerships. This includes

- Spouse (current and past)
- Siblings (including half siblings and their spouses)
- Children (including step-children and adopted children) and their spouses
- Parents (including step-parents)
- Grand children and their spouses

e. **Close Associates:** Individuals who are closely connected to PEPs either socially or professionally. This includes

- A natural person having joint beneficial ownership of legal entities and legal arrangements or any other close business relationship with a PEP
- A legal person or a legal arrangement whose beneficial owner is a PEP or an immediate family member or a close associate is a PEP.
- A publicly and widely known close business colleagues or personal advisors (specially those who are acting in a financial fiduciary capacity) of PEPs.

Procedure adopted at the Bank

Identification of PEPs

Acting in compliance with the regulatory framework it is proposed to consider following Persons/ Institutions as PEPs:

i. Local PEPs

- Present and former Presidents of the country
- Present and former Prime Ministers of the country
- Members of Parliament including Speaker and Deputy Speaker
- Members of Provincial Councils (including Governors of the Provinces), Members of Pradeshiya Sabas and Members of Municipal Councils.
- Leader, Secretary and Treasurer of all Political Parties
- Central Bank of Sri Lanka – Governor, Senior Deputy Governor, Deputy Governors and Assistant Governors and Heads and Additional Heads of the Departments.
- Auditor General's Department – Auditor General, Additional Auditor General and Assistant Auditor Generals.
- Diplomatic representatives of the government serving in foreign countries.
- Members of Monetary Board.
- Government appointed Commissions – Chairman, Members and Senior Officers.
- Senior Government Officials:
  - ✓ Government Departments – Director / Commissioner and above.
  - ✓ Corporations – General Manager and above.
  - ✓ Ministries – Additional Secretary and above.

- ✓ State Owned Enterprises – Head and Deputy Head of the entity.
- ✓ Statutory Boards – Head and Deputy Head of the entity.

- Judicial Officers
  - ✓ All judges.
  - ✓ Attorney General (AG).
  - ✓ Solicitor General and Additional Solicitor General of the AG's Department.
  - ✓ Registrars of Courts.

- Military Officers
  - ✓ Sri Lanka Army – Lieutenant Colonel and above.
  - ✓ Sri Lanka Air Force – Wing Commander and above.
  - ✓ Sri Lanka Navy – Commander and above.
  - ✓ Sri Lanka Police – ASP and above.

- Personal Secretaries, Coordinating Secretaries, Senior additional secretaries, Personal Relationship Officers and Media Secretaries to the President, Prime Minister and Cabinet Ministers; Personal and Coordinating Secretaries to Deputy/State/Provincial Council Ministers.

- Immediate family members and close associates of PEPs as detailed in the FIU Guideline.
- A private company where a PEP is a Director or a significant shareholder.
- Other Business concerns (Proprietorships, Partnerships) in which a PEP has a material interest/control.
- Any other person, who, in the opinion of the Bank should be categorized as a PEP based on information available in the public domain.

ii. Foreign PEPs

- Heads of Foreign States or Governments.
- Judges and Management Officials of International Courts, Judicial or Military officials.
- Heads/ Deputies/ Directors etc. of International Organizations.
- Members of international parliamentary assemblies.

iii. Duration of Treating a Person as a PEP

- Members of Parliament/ Provincial Councils/ Pradeshiya Sabas/ Municipal Councils immediate family members and close associates- as PEPs for life time

- Government/ Judicial/ Military officers, immediate family members and close associates- as PEPs only during the time they hold their offices and for a further period of six months after removal from office.

- Members, immediate family members and close associates of Government appointed Commissions/ Boards/ Corporations- as PEPs only during the time they hold their offices and for a further period of six months after removal from office.

iv. Identification of PEPs

PEPs shall be identified based on the customer self-declaration, information available in the PEP lists internally maintained at the Bank, information available in public domain and information available in the global watch lists.

v. Banking Relationships with PEPs

a. Opening New Accounts

The Bank has put in place a due diligence process on conducting banking relations with PEPs and as per the due diligence process

- The approval of the Senior Management (Deputy General Manager- Channel Management) should be obtained to open a new account for a PEP.
- Source of funds and wealth is identified through appropriate means
- PEP accounts are treated as High Risk in the customer risk profiling mechanism and they are subject to frequent periodic reviews.

b. Granting Facilities

Credit facilities to PEPs shall be granted with the prior approval of the Board of Directors.

vi. General Provisions

a. In accordance with the due diligence process implemented at the Bank all essential information such as principal occupation or employment, source of income, purpose of opening the account etc. shall be obtained to identify the customer.

b. Though middle ranking and junior individuals are not considered as PEPs, the Bank shall take measures to identify middle ranking or junior officials who act on behalf of PEPs to circumvent AML/CFT controls.

c. The Bank shall use the self-declaration, information available in public domain, information available in global watch lists, institutional websites etc. to identify international PEPs.

d. In order to identify the customers who have become PEPs after opening accounts with the Bank measures shall be taken to monitor non PEP accounts at instances where
   - a customer updates the Bank with information on his political exposure
   - ongoing monitoring reveals activities or information that suggests previously unknown political exposure
   - an election is held which effects any of the customer's PEP status
   - the Bank becomes aware of the need of such an update

e. If the Bank is of the opinion that the type of activities taking place in the account are not reasonable, when compared with the source of funds/ wealth, steps shall be taken to conduct a further assessment and a decision will be taken on continuation or termination of the business relationship and filing a suspicious transaction report with FIU o the findings of the assessment.

GLOSSARY

Beneficiary –

A person to whom or for whose benefit the funds are sent or deposited in or paid to a Financial Institution and may include a beneficiary Financial Institution.

Beneficiary Financial Institution –

An institution which receives wire transfers from the ordering institution directly or through an intermediary institution and makes the funds available to the beneficiary customer.

Beneficial Owner –

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 legal person or a legal arrangement.

Board of Directors –

In relation to a Financial Institution incorporated outside Sri Lanka means the senior management authority of such Financial Institution.

Customer –

In relation to a transaction or an account includes –

(a) The person in whose name a transaction or an account is arranged, opened or undertaken;
(b) A signatory to a transaction or an account;
(c) Any person to whom a transaction has been assigned or transferred;
(d) Any person who is authorized to conduct a transaction; or

(e) Such other person as may be prescribed.

Correspondent Banking –

Provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank) including cash management (*eg:* large international banks frequently act as correspondent banks for large number of other banks around the world by providing a wide range of services such as interest-bearing accounts in a variety of currencies, international wire transfers, cheque clearing, payable-through accounts and foreign exchange services).

Close Associate Includes –

(a) A natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship; and
(b) 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 family members.

Controlling Interest –

An interest acquired by providing more than ten percent (10%) of the capital of a Financial Institution.

Company Act –

The Companies Act No.7 of 2007.

Existing Customer –

A customer who has commenced a business relationship on or before these rules come into force.

Financial Action Task Force –

An independent inter-governmental body that develops land promotes policies to protect the global financial system against money laundering, terrorist financing and the financing for proliferation of weapons of mass destruction.

Financial Group –

A group of companies that consists of a parent company or other type of a legal person, exercising control and coordinating function over the rest of the group, for the application of group supervision under the anti-money laundering and suppression of terrorist financing policies and procedures, together with branches and subsidiaries that are subject thereto.

Finance Company –

A company licensed under the Finance Business Act No. 42 of 2011.

Immediate Family Member –

Includes the spouse, children and their spouses or partners, parents, siblings and their spouses and grandchildren and their spouses.

Intermediary Financial Institution –

An institution in a payment chain that receives and transmits a wire transfer on behalf of the Ordering Financial Institution and the beneficiary institution, or another intermediary institution.

Legal Person –

Any entity other than a natural person that is able to establish a permanent customer relationship with a financial institution or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association.

Legal Arrangement –

Includes an express trust, a fiduciary account or a nominee.

Licensed Bank –

Any commercial bank and specialized bank, licensed under the Banking Act No. 30 of 1988.

Majority- owned subsidiary –

A subsidiary of a group of companies of which fifty *percent* or more of the shares of the group of companies are owned by the parent company.

MVTS –

Financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message transfer or through a clearing network to which the relevant financial service provider belongs. Transactions performed by such service may involve one or more intermediary transactions and a final payment to a third party and may include any new payment methods.

Money Laundering –

The offence of money laundering in terms of section 3 of the Prevention of Money Laundering Act, No.5 of 2006.

Ordering Financial Institution –

An institution which initiates wire transfers and transfers the funds upon receiving the request for a wire transfer on behalf of the originating customer.

Person –

A natural or legal person and includes a body of persons whether incorporated or unincorporated and a branch incorporated or established outside Sri Lanka.

Politically Exposed Person –

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.

Payable through Account –

Correspondent accounts that are used directly by third parties to transact business on their own behalf.

Risk Based Approach –

In relation to the application of CDD measures to manage and mitigate money laundering and terrorist financing risks, means the use of simplified CDD measures in the case of customers with lower risk levels and the use of enhanced CDD measures in the case of customers with higher risk levels.

Shell Bank –

A bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective overall supervision. The physical presence constitutes being located within a country performing a management function with meaningful mind and the mere existence of a local agent or non-managerial staff does not constitute a physical presence.

Straight through Processing –

Payment, transactions that are conducted electronically without need for manual intervention.

Terrorist Financing –

An act constituting an offence connected with the financing of terrorism under the Convention on the Suppression of Terrorist Financing Act, No.25 of 2005.

ශ්‍රී ලංකා මහ බැංකුව
fNa0 It›{B M6uf5I
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය நிதியியல் உளவறிதல் பிரிவு **Financial Intelligence Unit**

Guideline No. 1/18

Ref: 037/05/002/0018/017

11" January 2018

To: CEO's of All Financial Institutions

Dear Sir/Madam,

Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. o6 of 2006 and the Financial Institutions (Customer Due Diligence) Rules, No. ol of 2016.

This guideline shall be treated as minimum instructions and indications to identify and assess the risk of Money Laundering & Terrorist Financing (ML & TF) in their businesses and take effective measures to mitigate the identified risk. It is important that all financial institutions will prepare their own risk assessment and mitigation report in line with this guidelines.

Yours Faithfully,

Director
Financial Intelligence Unit

Cc : Compliance Officer

14 වන මහල, අංක 30, ජනාධිපති මාවත, ¥4 @iâ iocq. g•c. ›o e +«@ud? +ocei@mg Qsc@fi›+j i Level ¥4 , Pa. 30, Jaiiadhipathl Maratha,
නැ. පෙ. 590, කොළඹ 01, ශ්‍රී ලංකාව த. பெ. இல. 590, கொழும்பு 01, இலங்கை P. O. Box. 590, Colombo 01, Sri Lanka.

94 14 2477125/509 94 11 2477692 fiu@cbsLlh www.fiusrilanha.Nov.ik

Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018

Introduction

1. The Financial Intelligence Unit of Sri Lanka (FIU), acting within the powers vested with it under the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA), issued the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 by Gazette Extraordinary No. 1951/13, dated January 27, 2016; effective from the date of issue, applicable to institutions which engage in "finance business" as defined under Section 33 of the FTRA.

2. As applicable under Rule 3 of the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016, the rules introduce, inter alia, provisions requiring financial institutions identified under the rules to take measures specified therein for the purpose of identifying, assessing, and managing Money Laundering (ML) and Terrorist Financing (TF) risks posed by its customers and business activities.

Risk Management

3. Every Financial Institution should identify and analyze ML/TF risks present within the financial institution and design and effective implementation of policies and procedures that are commensurate with and that mitigate the identified risks to ensure sound ML/TF risk management.

4. In conducting a comprehensive risk assessment to evaluate ML/TF risks, every financial institution should consider all the relevant risk factors present in its customer base, products, delivery channels and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business.

5. Risk assessments should be based on specific operational and transactional data and other internal information collected by the financial institution as well as external sources of

information such as national risk assessments conducted by Sri Lanka and by governmental agencies of foreign jurisdictions where the financial institution has business relationships, either through customers or branch/subsidiary networks, country reports from reliable international and regional organizations, such as reports and reviews prepared by the Financial Action Task Force (FATF), FATF-style regional bodies such as the Asia/Pacific Group on Money Laundering (APG), International Monetary Fund (IMF) and World Bank publications, and information from reliable commercial intelligence providers.

6. Financial Institutions are required to have a risk management framework to address ML/TF risks. Such a framework includes policies, controls and procedures that enable them to identify, measure, monitor, control and mitigate effectively the ML/TF risks that have been identified.

Risk Management Framework

Corporate Governance

7. The FIU expects financial institutions to establish a robust and effective corporate governance framework that ensures transparency, accountability and high ethical conduct in all aspects of their operations. Institutions should adopt a Code of Ethics that promotes consistently high standards of ethical conduct by all employees. A sound corporate governance framework includes the use of effective policies and procedures, monitoring and reporting mechanisms and internal controls. Measures that ensure appropriate separation of functions and the avoidance of conflicts of interests are essential hallmarks of an effective corporate governance regime. The Board of Directors (BoD) is ultimately responsible for establishing a corporate vision, strategy and business model and for overseeing an institution's corporate governance culture and is expected to develop mechanisms including board committees to achieve this objective. Senior management is responsible for ensuring the effective functioning of the corporate governance framework on a day-to day basis.

I. Board of Directors (BoD)

8. Members of the BoD should have a good understanding of the institution's business model and operations and the general business climate in which it operates. They should have the qualifications and experience necessary to understand the institution's business model and operations and how these relate to Sri Lanka's general economic and social environment. The BoD should ideally be comprised of both executive and non-executive directors to ensure a desirable level of independence from the institution's management function.

9. The BoD should establish the institution's overall risk appetite and should ensure that mechanisms are in place to effectively mitigate risk. The BoD must ensure that appropriate policies, procedures and controls are in place to manage such risks and should also ensure that arrangements are in place for the effective reporting on all issues related to the functioning of the risk management framework. The BoD is ultimately responsible for the institution's operations, its management of the risk to which it is exposed and its compliance with all laws, regulations and guidelines to which it is subject.

II. Senior Management

10. An institution's senior management is responsible for implementing the corporate vision, strategy and business model approved by the BoD. Senior management should demonstrate a firm understanding of all aspects of the institution's business model and is responsible for developing the components of the risk management framework. Senior management is responsible for ensuring that the institution has all the resources necessary to effectively manage risk. They are also responsible for ensuring that effective communication and reporting arrangements are in place to support good risk management practices. This includes ensuring that all staff members are aware of the requirements of the risk management framework and their specific roles and responsibilities. Senior management is responsible for ensuring that internal reporting mechanisms, including reports to be sent to the BoD, are developed to provide accurate and timely information relevant to the effective management of risks.

The Risk Management Function

11. The FIU expects institutions to develop an effective risk management function. The risk management function responsible for ensuring that the institution effectively identifies, measures, monitors, and controls and mitigates risks. From a day-to-day operational perspective risk management supports senior management and the BoD to achieve the ML/TF risk management objectives discussed in this guidance note. The risk management function should be commensurate with the, size, nature and complexity of the institution's business model and operations.

Policies and Procedures

12. The FIU expects the senior management to develop policies and procedures to effectively manage the ML/TF risks that arise from an institution's operations. Policies and procedures developed by senior management should be approved by the BoD. Policies and procedures should set out the day-to-day measures that should be employed to ensure that the institution effectively identifies, measures, monitors and controls ML/TF risks. They should therefore be developed to reflect the risks implicit in an institution's customers, products and services, delivery channels and geographic regions. Policies and procedures should be comprehensively documented and communicated to all staff. They should also be subject to periodic review to ensure they are appropriate in light of changes to the institution's ML/TF risk profile.

13. Policies and procedures should clearly set out lines of responsibility and accountability for the execution of the risk management function and should also establish effective reporting lines for all persons and business units involved in the management of ML/TF risks.

14. An effective risk management framework should establish limits in the context of the institution's stated appetite for ML/TF risk and the overall effective implementation of the risk management system. Policies and procedures should limit, for example, an

institution's exposure to the ML/TF risks arising from exposure to specific types of customers, products and services, delivery channels and geographic regions. An effective ML/TF risk management framework should include a mechanism to report incidents where established limits have been breached and the frequency of such events.

Internal Controls

15. An on-going system of internal controls is an essential component of a risk management framework. Institutions are expected to employ measures on an on-going basis to ensure adherence to establish policies and procedures as well as relevant laws, regulations and guidelines.

16. Arrangements should be in place to reinforce the "four eyes" principle and avoid conflicts of interest. Measures should be employed, for example, to ensure adequate separation between operational and control functions such as front office and back office activities.

17. Institutions are expected to develop effective internal audit arrangements. The internal audit function should be an independent function with a direct reporting line to the Board Audit Committee. The internal audit function should periodically assess the effectiveness of the institution's ML/FT risk management framework and practices paying specific attention to the institution's adherence to established policies procedures and limits and applicable laws, regulations and guidelines.

18. Institutions are also expected to ensure that their ML/TF risk management framework and practices are subject to external audit review.

The Compliance Function

19. The FIU expects institutions to develop an effective compliance function as a component of its ML/TF risk management framework. The compliance function should be commensurate with the, size, nature and complexity of the institution's business model and

operations. The compliance function is separate from the internal audit function as it is a component of an institutions day-to-day operational activity. The compliance function should on an-ongoing basis assess the extent to which the institution is complying with established policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines. The effectiveness of the compliance function rests heavily on the effectiveness with which the Mangement Information System (MIS) generates accurate and timely reports related to the management of ML/TF risks. Compliance officer should possess sufficient seniority and knowledge and be up to date with recent laws and regulations

Risk Monitoring and Reporting

20. To effectively control and mitigate risk, institutions may need to develop MIS systems that provide reliable data on the quantity and nature of ML/TF risks and the effectiveness with which risks are being mitigated. The MIS system used by an institution should be commensurate with the size, nature and complexity of its business model and operations. Such systems should constantly measure ML/TF risks, changes to the nature of such risks and should also report on adherence to the policies and procedures designed to mitigate risks. The system should, for example, not only identify instances in which policies and procedures have been breached but should maintain a record of all such incidents. The system should provide timely reports to all business units and senior management to allow them to make judgments on the measures necessary to manage risks. Reports should also be prepared and submitted to senior management and the BoD indicating how well the institution is managing risk and highlighting instances of breaches of risk management policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines.

Training

21. The FIU expects institutions to have effective arrangements in place to train their staff on all issues related to their AML/CFT regime. It is important that staff understand the institution's inherent ML/TF risks and the nature of the measures that have been developed

to mitigate these risks. Training must be provided for all staff upon joining the institution and should be an-ongoing activity. Apart from general training provided to all staff, targeted training programs should be developed for specific categories of staff in light of the nature of their work in the context of ML/FT risks. AML/CFT awareness raising programs should be conducted for members of the BoD.

Assessing ML/TF Risk – Some Guidance

22. The following guidance sets out a methodology for the conduct of an assessment of ML/TF risks by a financial institution. It is not mandatory to follow this methodology, however, the FIU requires that each financial institution should undertake a comprehensive assessment of its ML/TF risks and develop appropriate risk management processes.

I. Identification of Vulnerabilities:

23. Financial Institutions are required to take appropriate steps to identify aspects of their business activities, including types of customers and transactions, which may be vulnerable to ML/TF and should in doing so, take into account the findings of the National Money Laundering and Terrorist Financing Risk Assessment of Sri Lanka[1]. Financial institutions should consider the following areas when identifying risk factors of their business that make them susceptible to ML/TF.

i. The nature, size and complexity of the business

The size and complexity of a financial institution plays an important role in how attractive or vulnerable it is for ML/TF. For example, a large financial institution is less likely to know its customers personally and this could offer a greater degree of anonymity to customers than a smaller financial institution.

[1] A copy of this report can be found at the FIU's website, http://www.fiusrilanka.gov.lk/docs/Other/Sri_Lanka_NRA_on_ML_2014_-_Sanitized_Report.pdf

Similarly, a financial institution that conducts complex transactions across international jurisdictions could offer greater opportunities for ML/TF than a purely domestic business.

ii. The products and services the business offers

Some products and services are more attractive for ML/TF. When considering whether the products and services the business offers could be susceptible or attractive for ML/TF, the following is a list of indicators (not exhaustive) that identifies ML/TF risk arising from products and services that are commonly offered by financial institutions.

- private banking services such as prioritized or privileged banking
- credit/ debit and other top-up cards
- non- face-to-face business relationship or transaction
- payment received from unknown or unrelated third parties
- any new product & service developed
- services to walk-in customers
- mobile banking
- single premium insurance policy

iii. The types of customers the financial institution deals with

Listed below are some indicators (not an exhaustive list) to identify ML/TF risk arising from customers.

Categories of customers pose a higher risk of ML/TF can include:

- new customers that wish to carry out a large transaction(s)
- non face-to-face customer on-boarding
- customers involved in occasional or one-off transactions above the threshold (either specified in the FTRA, the Customer Due Diligence (CDD) Rules or the financial institution's internal limits)
- customers who use complex business structures that offer no apparent financial benefits

- customer or a group of customers making numerous transactions to the same individual or group
- customers who are Politically Exposed Persons (PEPs)
- customer who has a business which involves large amounts of cash
- customer whose identification is difficult to check
- customer who bring in large amounts of used notes and/or small denomination notes.
- customers conducting their business relationship or transactions in unusual circumstances for example: significant and unexplained geographic distance between the financial institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations
- non- resident customers
- corporate customers whose ownership structure is unusual and excessively complex
- customers whose origin of wealth and/or source of funds cannot be easily verified or where the audit trail appears to be broken and/or unnecessarily layered
- customers that are non-profit organizations
- customers who conduct business through or are introduced by "gatekeepers" such as accountants, lawyers, or other professionals
- customers of a type that have been identified in National or Sector Risk Assessments as higher risk

iv. the countries that the financial institution deals with

Financial institutions should give consideration to the following factors as indicators of higher risk for ML/TF:

- any country subject to United Nations sanctions embargoes or similar measures
- any country identified by credible sources such as the FATF as lacking adequate AML and CFT system
- any country which is identified by credible sources as having significant level of corruption, tax evasion, and other criminal activity
- any country identified by credible sources as supporting TF

- any country that are identified by credible sources as tax havens

v. the business delivery methods or channels

The way the financial institution delivers its products and services affects its vulnerability to ML/TF.

The following are some indicators (not an exhaustive list) that may help to identify ML/TF risk involved with business delivery methods or channels

- non-face-to-face customers (via post, telephone, internet,) that pose challenges for verifying the identity of the account holder/customer.
- indirect relationships with customers (via intermediaries, gatekeepers, pooled accounts)

II. Risk Assessment

24. Having identified the threats involved, financial institutions need to assess and measure ML/TF risk in terms of the likelihood (chance of the risk event occurring) and the impact (the amount of loss or damage if the risk event occurs). The risk associated with an event is a combination of the likelihood that the event will occur and the seriousness of the damage it may do.

Likelihood scale

25. A likelihood scale refers to the potential of an ML/TF risk occurring in the business for the particular risk being assessed. Three levels of likelihood of ML/TF risk are shown below, but financial institutions can have as many scales as are necessary for their circumstances.

i. Very likely - Almost certain;
ii. Likely- High probability;
iii. Unlikely- Low probability, but not impossible.

Impact scale

26. An impact refers to the seriousness of the damage that is likely to be caused if the ML or TF occurs. In assessing the possible impact or consequences, the assessment should be made from a range of viewpoints relevant to the business. Those set out below are not exhaustive. The impact of ML/TF occurring could, depending on the individual financial institution and its business circumstances, be rated or looked at from the point of view of:
    i. how it may affect the business in terms of financial loss relating to market perceptions (for example loss of investor confidence) and reputation or through fines or other sanctions (such as loss or suspension of business licenses) imposed by a regulator
    ii. the risk that a particular transaction may be seen to contribute to the activities of a terrorist or terrorist organizations.
    iii. the risk that a particular transaction may result in funds being used for any unlawful activity as defined in Section 33 of the FTRA
    iv. how it may affect the reputation of the financial institution if it is found to have aided, investigated, prosecuted or otherwise implicated in an illegal act, which may lead to loss of important commercial relationships (such as correspondent accounts) or being shunned by the community of customers or shareholders/investors

27. Three levels of impact of an ML/TF risk to financial institutions are shown below as an example. However, the FIU encourages financial institutions to develop their own ML/TF risk processes and assessments for dealing with certain customers/undertaking transactions in the way that best suits their business model/activities.
    i. Major- significant consequences, that inflict substantial damage, possibly resulting in the closure of the financial institution, cessation of business activities, regulatory sanctions being imposed or financial/reputational damage being experienced by the financial institution which will have a significant impact on business activities.
    ii. Moderate- moderate impact, involving substantial damage to the business and its reputation.
    iii. Minor- minor or negligible consequences or effects upon the financial institution.

28. Based on the likelihood and impact scale, it is suggested that financial institutions should assess an overall risk score. The risk rating may be used to aid decision making and help in deciding what action to take in view of the overall risk. A suggested risk rating derivation can be seen in the risk matrix *(Annex 1)*. However, institutions are encouraged to adopt their own approach to assessing, identifying and quantifying ML/TF risk. Irrespective of the methodology adopted, the FIU requires institutions to develop a framework and implement practices to effectively identify, measure, monitor, control and mitigate ML/TF risks as required by the FTRA and CDD Rules.

i. Extreme - risk almost certain to happen and/or to have very serious consequences on the financial institution, including its financial standing and reputation.
   Response: Do not allow transaction to occur/or customer relationship to be established or reduce the risk to acceptable level through risk mitigation, such as enhanced due diligence.
ii. High - risk likely to happen and/or to have serious consequences.
   Response: Do not allow transaction/establishment of customer relationship until risk reduced through risk mitigation, such as enhanced due diligence.
iii. Medium - possible this could happen and/or have moderate consequences.
   Response: Mitigate risk; normal CDD and other requirements apply.
iv. Low - unlikely to happen and/or have minor or negligible consequences.
   Response: Mitigate risk: simplified CDD and other requirements apply.

III. Risk Mitigation

29. Once the financial institution assesses the ML/TF risk of individual customer, product/service, delivery channel and risks related to geographic region, it should develop strategies policies and procedures to manage and mitigate the risk.

Examples of a risk reduction or mitigation are:

i. Setting transaction limits for high-risk products or delivery channels

ii. Having a management approval process for higher risk customers, products, services, or deliver channels

iii. Risk rating customers and applying different requirements for high or low risk customers including applying different identification and verification methods and enhanced customer due diligence requirements

iv. Not accepting customers who wish to transact with a high-risk country or customers that are considered to be higher risk based on the institution's board-approved customer acceptance policy.

Risk Management Strategies

30. Financial institutions shall adopt the following components, among others, as part of their risk management strategy:

i. Develop and implement ML/TF risk management objectives at the board and senior management level of the financial institution and monitoring progress of implementation of objectives.

ii. Implement clearly defined management responsibilities and accountabilities regarding ML/TF risk management.

iii. Provide adequate staff resources to undertake functions associated with ML/TF risk management.

iv. Introduce staff reporting lines from the ML/TF risk management system level to the board or senior management level, with direct access to the board members or senior managers responsible for overseeing the system.

v. Implement procedural controls relevant to particular services and products, customers, and delivery channels that have been identified as being vulnerable to ML/TF.

vi. Documenting all ML/TF risk management policies and ensuring that these are kept up to date and reviewed regularly reflecting both the scope and nature of the institution's activities and the findings of risk assessments conducted by authorities. Such policies should also identify processes relating to non-compliance, including reporting of suspicious transactions to the FIU.

vii. Provide appropriate training programs for staff to develop expertise in the identification of ML/TF risks across the financial institution, including reporting of suspicious transactions.

viii. Develop an effective information management system which produce detailed and accurate financial, operational and compliance data relevant to ML/TF risk management.

Enhanced and Simplified Due Diligence Measures

31. There are circumstances where the risk of ML/TF is higher and enhanced CDD measures must be taken and, where the risks of ML/TF are lower, simplified CDD measures may be taken. These enhanced and simplified measures are outlined below:

Enhanced due diligence measures for high risk customers/transactions

32. Every financial institution should examine and document, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of ML/TF are higher, financial institutions should be required to conduct enhanced due diligence (EDD) measures for higher-risk business relationships which may include:

i. Obtaining and verifying additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet search, etc.)
ii. Updating more regularly the identification data of customer and beneficial owner
iii. Obtaining and verifying additional information on the intended nature of the business relationship
iv. Obtaining and verifying information on the source of funds or source of wealth of the customer
v. Obtaining and verifying information on the reasons for intended or performed transactions
vi. Obtaining and verifying the approval of senior management to commence or continue the business relationship
vii. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
viii. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures for low risk customers/transactions

33. Where the risks of ML/TF are lower, the financial institutions are, subject to the regulations, allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring).

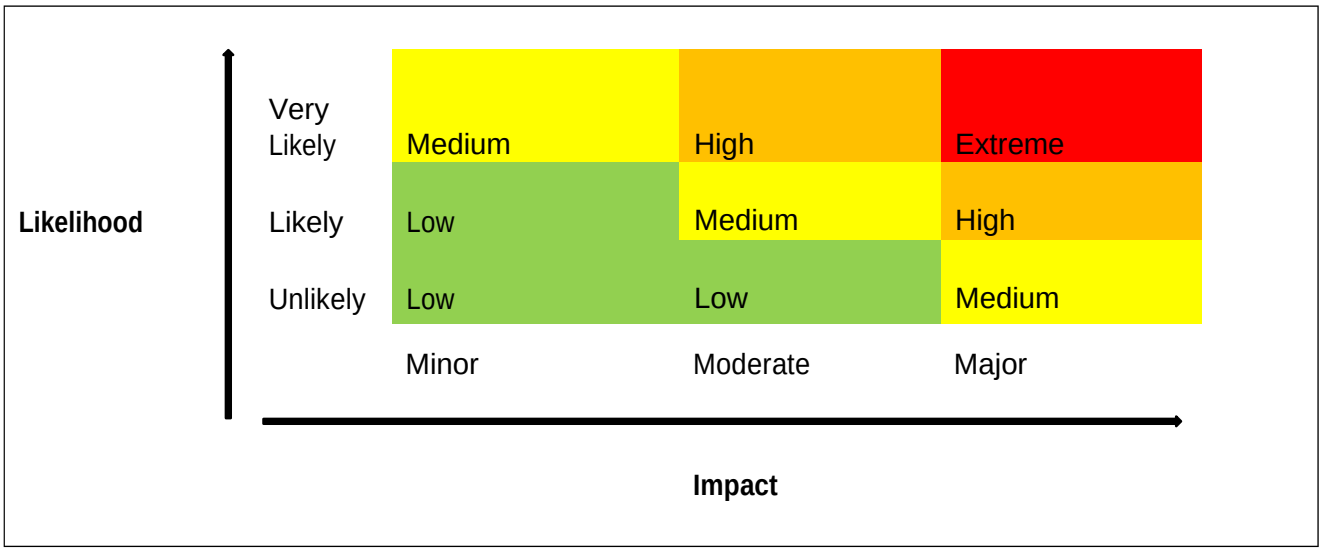
Examples of possible measures are:

i. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (delayed verification)
ii. Reducing the frequency of customer identification updates
iii. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
iv. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established

34. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF, or where specific higher-risk scenarios apply.

Annex 1

Overall AML/CFT Risk



CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය நிதியியல் உளவறிதல் பிரிவு **Financial Intelligence Unit**

Ref : 037/03/011/0001/018

Guidelines — 06/2018

August 06, 2018

To: CEOO of All Financial Institutions

Dear Sir / Madam,

Guidelines for Financial Institutions on Suspicious Transactions Reporting,
No. 06 of 2018

The above mentioned guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 and the Suspicious Transactions (Format) Regulations of 2017.

Yours faithfully

D M Rupasinghe
Director
Financial Intelligence Unit

Cc : Compliance Officers

14 වන මහල, අංක 30, ජනාධිපති මාවත, නැ . පෙ . 590, කොළඹ 01, ශ්‍රී ලංකාව
1 94 11 2a77125/509 t" 94 11 2477G92

14 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை கொழும்பு 1
த. பெ. இல. 590, கொழும்பு 01, இலங்கை
@ fi«ecbsLik

Level 14 , No. 30, Janadhipathi Mawatha,
P . O. Box. 590, Colombo 01, Sri Lanka.
www.cbsl.gov.lk

Guidelines for Financial Institutions on Suspicious Transactions Reporting, No. 06 of 2018

Introduction

1. These Guidelines are issued pursuant to section 15(1)(j) of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) applicable to Financial Institutions that engaged in or carrying out "finance business" as defined in Section 33 of the FTRA.

2. Suspicious Transactions (Format) Regulations of 2017 was issued on dated April 21, 2017 by Gazette Extraordinary No. 2015/56 applicable to Institutions which include institutions that engaged in or carrying out "finance business" as defined in Section 33 of the FTRA. These Guidelines are provided as an aid to interpret and apply Suspicious Transactions (Format) Regulations of 2017. These Guidelines are not intended to be exhaustive and do not constitute legal advice from the Financial Intelligence Unit (FIU). Nothing in these Guidelines should be construed as relieving Financial Institutions from any of their obligations under the Suspicious Transactions (Format) Regulations of 2017 or the FTRA.

3. The quality of a Suspicious Transaction Report (STR) is important in increasing the effectiveness of the quality of analysis and investigations undertaken by FIU and law enforcement agencies relating to such STR which would assist in preventing abuse of the Sri Lankan financial system by criminals and terrorists. Quality, in this sense, means reports should be based on results from an AML/CFT programme that is effectively implemented and that the content in reports are complete, accurate and latest. This guideline aims at assisting Financial Institutions in improving the quality of STRs submitted.

Legal Obligation

4. Section 7 of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) requires:

   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. 5 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 therefrom, report the transaction or attempted transaction or the information to the Financial Intelligence Unit.

Such reports are herein referred to as Suspicious Transaction Reports (STR).

5. As stated above as per the section 7 of the FTRA all "Institutions", should report suspicious transactions to the FIU. Institution means, any person or body of persons engaged in or carrying out any finance business or designated non-finance business as defined in the Section 33 of the FTRA.

6. As per Section 14 (1) (b) (iv) of the FTRA every institution is required to establish and maintain procedures and systems to implement the reporting requirement under Section 7 of the FTRA. Further, Section 14 (1) (d) requires every Institution to train its officers, employees and agents to recognize suspicious transactions.

7. As per Rule 15 of the Financial Institutions Customer Due Diligence Rule, No 1 of 2016, the internal AML/CFT Policy approved by the Board of Directors should include policies, procedures on the detection and internal reporting procedure of unusual and suspicious transactions and the obligation to report suspicious transactions to the Financial Intelligence Unit.

Prerequisites for Development of Suspicion

8. Reporting of suspicious transactions is a major functionality in the operation of an effective institutional AML/CFT programme. For the AML/CFT function to be meaningful, they must result from a Financial Institution's effective implementation of the FTRA, including all rules and instructions issued in relation to the FTRA. Financial Institutions without such effective implementation either tend to submit STRs that are inaccurate, incomplete or inappropriate or they may fail to report suspicious transactions entirely. Such failures expose the financial institution to regulatory, reputational, operational, and legal risks. In some cases, such failures may also expose both natural and legal persons to criminal liability.

9. For all but the very smallest institutions with the most intimate customer relationships, information about customers and transactions should be captured in a systematic manner and incorporated into their compliance and risk management processes. For larger Financial Institutions, this almost always means an electronic information

system. Such systems typically operate based on rules, scenarios and profiles that seek to measure and assess deviance of observed patterns from expected patterns, or seek to measure and assess conformity of observed patterns to known patterns of abuse of the financial system. Such systems need to be carefully configured to reflect the specific assessed risks of the Financial Institution. Such systems need to be continually evaluated and adjusted to maximize effectiveness, need to be continually updated with new operational and third-party information and need to be fully integrated into the Financial Institution's risk management process. When such systems generate alerts, it is important that the alerts are reviewed by the Financial Institution's Compliance Officer. While such system-generated alerts may be the cause for an STR, such alerts are not by themselves likely to form a complete STR in accordance with these guidelines and are not an acceptable substitute for such an STR.

Systems that operate in isolation are not effective. A system can only operate based on the information that is available to it. Systems are not generally capable of intuition or inference or human levels of perception. As such systems operate based on rules, scenarios and profiles that are designed by humans. For these reasons, Financial Institutions should not rely exclusively on systems to the exclusion of human involvement.

10. Whatever the source of customer and transaction knowledge, and whatever the technical sophistication of the AML/CFT system there must be an institutional will to make the system work. That is, there must be a will to detect suspicious transactions, to recognize in good faith such suspicious transactions for what they are when detected, and fully and accurately report such transactions, when recognized. Such institutional will is most effectively created by a commitment from those at the Senior Management including the Board of Directors of the Financial Institution and propagated through concrete actions and demonstrations (e.g. development of effective internal policies, processes and training programmes, compliance audits, investment in systems, consistent, fearless and disciplined exercise of judgment) to the rest of the staff of the Financial Institution.

Suspicion

11. Financial Institution must develop its own operating definition for suspicion. A Financial Institution's operating definition of suspicion should incorporate elements of unresolved and unsubstantiated but persistent feelings of doubt about an objective set of facts and circumstances relating to a behaviour, to a single transaction, to a series of transactions, attempted transaction or to any combination thereof. It can be a feeling that something is not as it was expected to be, or as it was explained to be, given the totality of knowledge of the circumstances in which that something exits. The feeling of doubt cannot be relieved by proof, one way or another, since no proof is available. The definition should allow formation of a belief that is not firmly grounded or perfectly

clear. At the same time, the definition should not allow these beliefs to be fanciful or fleeting. Certainly, the definition should count as suspicious behaviours and activities that are unusual for the circumstances and not adequately or believably explained.

The operating definition for suspicion must pass a test of reasonableness. If the definition is too narrow or rigid, it may exclude generation of reports that concern unknown or unanticipated unlawful circumstances (i.e. “false negatives”) and may also result in avoidance behaviour by criminals. On the other hand, a definition that is too broad or flexible might result in large number reports that are insufficiently analyzed and that do not reflect unlawful circumstances (i.e. “false positives” or “over compliance”). For Financial Institutions where electronic information systems are integrated into their processes, operating definitions are partially implemented by the triggers, profiles, scenarios and rules defined by the Financial Institution. Suspicious indicators and typologies may also be elements of such definition. The concept of “unusual” patterns of behaviour and transactions should also reflect in these definitions.

A non-exhaustive and unofficial list of suspicious indicators for transactions and behaviours is provided in Appendix I. The Financial Institution should complement this list with the Financial Institution’s own indicators. When using indicators, it should be remembered that these indicators are not formulae and they do not necessarily indicate the presence of criminality. Conversely, the lack of known indicators does not necessarily mean the absence of criminality, in part because criminals may adjust behaviour to avoid such indicators. Instead, indicators, and especially combinations of indicators, should cause increased scrutiny that may lead to the formation of suspicion.

12. Financial Institutions being over compliance or malicious compliance will not generate expected quality of the STR. Overcompliance and malicious compliance are strongly discouraged.

    Over compliance results when Financial Institutions submit a large volume of reports that are inadequately analyzed or that fail to meet a reasonable standard of suspicion. Over compliance can be viewed as an attempt to transfer risk management from the Financial Institution to the FIU.

    Malicious compliance is when an Financial Institution submits reports that, although they may contain some superficial elements of suspicion, are known by the Financial Institution to not actually of suspicious nature.

13. If after consideration of facts and circumstances available to the Financial Institution in good faith and within the context of the Financial Institution’s own understanding of suspicion and risks for the Financial Institution, and after gaining a thorough understanding of the FTRA and its implementing rules, regulations, circulars and guidelines, the Financial Institution has doubts about whether a behaviour or activity should be reported as suspicious, the best course of action is to report.

Reporting of STRs

14. **When Financial Institutions are provided with access to the LankaFIN system:** All reports must be submitted via LankaFIN online system or a successor system designated by the FIU followed by the signed hard copy of the STR submitted to the FIU by delivery or post.

15. **When Financial Institutions are not provided with access to the LankaFIN system:** Signed hard copy of the STR should be submitted to the FIU by delivery or post.

16. The Financial Institutions may submit STRs through other forms such as by way of email, fax or telephone in urgent situations to be followed by submission though LankaFIN and/or signed hard copy as appropriate within twenty-four hours.

Timing of Reporting

17. The FTRA requires suspicious reports to be submitted to the FIU as soon as practicably possible but no later than two working days of formation of suspicion. This means that, regardless of the Financial Institution's processes, procedures and steps after the initial formation of suspicion, the suspicion itself must be reported even if the Financial Institution's process has not completed. The Financial Institution's process for dealing with suspicion may proceed concurrently with the reporting of suspicion.

    For example, if the Financial Institution has a customer that receives a wire transfer in circumstances that the Financial Institution immediately considers to be suspicious, the Financial Institution must report the suspicious circumstances of that transaction as soon as practicable but within two working days even while the Financial Institution may continue with the internal processes that to verify the authenticity and details of the wire transfer.

18. If, after sending the report, the Financial Institution discovers additional facts and circumstances to either support or refute the Financial Institution's initial suspicion, then the Financial Institution should inform the FIU appropriately.

Content of Reporting

19. **Completeness:** A single STR must stand alone and contain complete information about the suspicion. A STR should provide a full picture of the suspicion itself as well as the objective facts and circumstances that gave rise to and support that suspicion. Where multiple transactions and/or behaviours are connected with a suspicion, a single report should be filed capturing all of these.

20. **Form Narrative:** The narrative portion of the report is most important. This is particularly true with respect to LankaFIN since other form fields capture only a limited amount of information. This is the Financial Institution's chance to fully describe the suspicion and the objective facts and circumstances that gave rise to and support the Financial Institution's suspicion. In any case the Financial Institution is unable to provide the full detailed narrative through LankaFIN, the Financial Institution may provide the narrative in a separate document and submit to the FIU along with the signed hard copy of the STR. In such cases, the Financial Institution should mention a brief summary of the narrative in the LankaFIN system and explicitly mention that a full narrative will be sent with the hard copy. The narrative should attempt to answer to the extent possible the basic descriptive questions of **what, who, when, where, why and how**.

    Financial Institutions should refrain from providing vague details of suspicions such as 'several high value third party deposits from several branches around the country'. Instead, Financial Institutions should provide clear quantitative and qualitative data such as '10 number of third party deposits having values between LKR 75,000 – 90,000 from Jaffna, Trincomalee, Kandy, Matara, Galle, Kataragama and Badulla branches during September, 2017' and provide relevant supporting documents (e.g. account statement for September 2017 including the details of third party depositors / deposits).

    Some of the questions that the narrative should attempt to answer, if possible, include:

    - What is the nature of the suspicion?
    - What offenses may have been committed?
    - What transactions, attempted transactions, behaviours, facts, belief and circumstances are involved and relevant to the suspicion?
    - Who are the natural and legal persons involved?
    - Who are the beneficial owners?
    - What are their identifiers such as names, ID numbers, registration numbers, etc.?
    - What are their addresses?
    - What are their occupations or lines/types of business?
    - Who are their employers?
    - What political exposure do they have, if any?
    - How are they connected with each other and with the transactions?
    - What were their roles in the transactions?
    - What property is involved?
    - What is the nature and disposition and estimated value of involved property?
    - When and where did the transactions or attempted transactions or behaviours occur?

- How, if at all, do the timing or location of the transactions contribute to the Financial Institution's suspicion?
- Why do these facts and circumstances support the suspicion?
- How was the suspicion formed?
- What triggers or indicators are present?
- What actions have been taken by the reporting Financial Institution?
- What related STRs have the Financial Institution already submitted?
- What red flags are present?
- What deviations from expected activities have taken place?

Financial Institutions are required to provide reasonable grounds for the suspicion and are requested to refrain from citing unjustifiable reasons such as 'relationship between customers cannot be derived with the surnames', 'funds from African countries', etc.

The narrative should be structured in a logical manner so that information can be conveyed to the FIU analyst as efficiently, completely and accurately as possible. Essay formats could be used for STR narratives i.e. having an introduction, a body, and a conclusion. Paragraph breaks can be used to divide the narrative into logical units and enhance readability. Within the body, information could be presented in a chronological manner when attempting to demonstrate possible causal links along a timeline. It is advised to minimize the use of Financial Institution's internal jargon and acronyms brandings, product names by using generic descriptors instead. For example, use "six-month term deposit account" rather than "Mega-Six Platinum Elite Plus Super Saver Account." Use punctuation and sentence case. Narrative should not be so brief as to compromise the goals of the narrative. It is advised to avoid words that do not contribute to the meaning of a sentence and to refrain from using too generic narratives such as 'the transaction pattern does not match with the customer profile'.

21. **Accuracy:** It is imperative that factual information provided in the report is accurate. This is particularly true for identifiers such as names, ID numbers, registration numbers, etc. All spellings and transcriptions of identifiers should be double checked. A single inaccurate digit in a passport number or an NIC, or a misplaced or transposed character in a name, can make the difference between a successful and an unsuccessful analysis. Identifiers for legal entities (e.g. company / business registration number, registered name of company) should be exactly identical in every respect to those found on the official registration documents.

Submission of Supporting Documents

22. Financial Institutions are required to submit relevant supporting documents along with the STR. If the Financial Institution is unable to submit the supporting documents via LankaFIN, the Financial Institution should submit the relevant supporting documents

through email and/or along with the signed hard copy of the STR. In such cases, Financial Institutions should mention in LankaFIN that additional supporting documents are submitted via email or through post.

23. Supporting documents should support rather than replace the STR contents, including the narrative. It is not acceptable to only refer to a supporting document in the narrative when information from the supporting document can be directly included in the narrative. For example, if the suspicion involves a letter of credit, all the details from the letter of credit that are related to the suspicion should be included in the narrative. A copy of letter itself can then be provided as a supporting document.

24. An indicative and non-exhaustive list of supporting documents along with corresponding scenarios are given below for reference.

Scenario	**Indicative list of Supporting documents**
Third party deposits	Bank Statements List of third party deposits Details of third party depositors
Foreign inward remittance	Bank statement Copy of SWIFT message
Suspicion regarding forged / altered identity (NIC/ Passport / Driving license)	Copy of the document
Suspicion related to a company	Registration documents Director details

Miscellaneous

Confidentiality

25. As per the Section 9 of the FTRA Financial Institutions are not allowed to inform any person, including the customer, about the contents of an STR and even that the Financial Institution has filed such a report to the FIU.

26. As per Rule 46 of the Financial Institutions Customer Due Diligence Rule, No. 1 of 2016, where a Financial Institution forms a suspicion of money laundering or terrorist financing risk relating to a customer and where the Financial Institution reasonably believes that conducting the process of CDD measures would tip off the customer, then the Financial Institution should terminate conducting the CDD measures and proceed with the transaction and immediately file an STR.

Breach of Confidentiality

27. If any customer is being tipped off about the reporting of STRs by any officer of the Financial Institution it would consider as a violation under the FTRA Section 9 and 10. This is described as the offence of 'tipping off' and is an offence punishable with a fine not exceeding five hundred thousand rupees or imprisonment of either description for a term not exceeding two years, or to both such fine and imprisonment.

Protection for Persons Reporting STRs

28. As per Section 12 of the FTRA:
    No civil, criminal or disciplinary proceedings shall lie against —
    (a) a such Institution, an auditor or supervisory authority of an Institution ; or
    (b) a director, partner, an officer, employee or agent acting in the course of that person's employment or agency of an Institution, firm of auditors or of a supervisory authority, in relation to any action by the Institution, the firm of auditors or the supervisory authority or a director, partner, officer, employee or agent of such Institution, firm or authority, carried out in terms of the FTRA in good faith or in compliance with regulations made under this Act or rules or directions given by the Financial Intelligence Unit in terms of the FTRA.

Failure to Report STRs

29. If a Financial Institution fails to submit STRs when reasonable grounds exist to suspect that a transaction is related to money laundering or terrorist financing, such is considered as non-compliance with the FTRA. As per Section 19 of the FTRA such non-compliances are liable to penalties up to one million rupees (Rs. 1,000,000.00) or double this for subsequent failures to report.

Should a reporting entity continue a business relationship with a customer about whom a STR has been reported?

30. The FTRA does not prohibit Financial Institutions from continuing business relationships with customers about whom STRs has been reported or suspicion has been formed. Especially Financial Institution's behaviour toward the customer should not amount to any tipping off subject to the provisions of the Section 3 of the FTRA.

Obligations of Financial Institutions which has submitted an STR in relation to a customer and is continuing the business relationship

31. After the submission of an initial STR, the Financial Institution should continue to comply with all relevant provisions of the FTRA in all future dealings with that customer, which may include a requirement to submit additional STRs /information on further suspicions identified / further developments.

Further Information Requests

32. Where the FIU has requested further information regarding any STR, the Financial Institution should take all necessary measures to provide such information promptly to the FIU.

Appendix I—Suspicious Indicators

This appendix contains a list of indicators related to customer behaviours and activities. This list is necessarily non-exhaustive and incomplete and should be modified and supplemented as necessary by each Financial Institution. Indicators are not formulae and they do not always indicate the presence of criminality. Conversely, the lack of indicators does not mean the absence of criminality. **However, the presence of an indicator, and especially the presence of multiple indicators, should cause increased scrutiny by the Financial Institution and such scrutiny may lead to the formation of suspicion.**

General Indicators

- Any behaviour unusual for the circumstances.
- Any activity unusual for the customer.
- Any activity unusual in itself.
- Any knowledge that leads the Institution to believe that unlawful activity may be involved.
- Any unresolved and persistent feelings of doubt related to customers and their transactions and attempted transactions.

General Behavioural/Customer Indicators

- Customer talks about or hints about involvement in criminal activities, even if in a humorous way.
- Customer does not want correspondence sent to home address.
- Customer appears to have accounts with several financial institutions for no apparent reason.
- Customer repeatedly uses an address but frequently changes the names involved.
- Customer uses addresses in close proximity of each other.
- Customer is accompanied and watched when visiting the Financial Institution.
- Customer shows unusual curiosity about internal systems, controls and policies.
- Customer has only vague knowledge of the amount of a deposit.
- Customer presents confusing or inconsistent details about the transaction.
- Customer over justifies or explains the transaction.
- Customer tries to convince Financial Institution staff to alter or omit reporting data.
- Customer is secretive and reluctant to meet in person.
- Customer is nervous, not in keeping with the transaction.
- Customer insists that a transaction be done quickly.
- Customer attempts to develop a close rapport with staff.
- Customer offers money, oversized commissions, gratuities or unusual favours for the provision of services.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer jokes about needing or not needing to launder funds.
- Customer has no apparent ties to the community.
- Customer has irregular work/travel patterns.

Account Opening/Identity Indicators

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer only possesses copies of personal identification documents.
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customer's supporting documentation lacks important details.
- Customer unnecessarily delays presenting corporate documents.
- All identification presented is foreign or otherwise unreasonably difficult to verify.
- All identification documents presented appear new or have recent issue dates.
- Customer is unemployed, or is an independent consultant, or switches jobs frequently.
- Customer conspicuously displays large amount of cash.

Indicators for a Businesses

- Lack of regular business hours.
- Unusually profitable business.
- Profitable business in a failing industry.
- Business receipts and incomes above industry norms.
- Cash intensive business.
- Use of high cost or inconvenient methods when lower cost or more convenient methods are available.
- Apparent lack of in-depth knowledge of his own business or industry.

General Transaction Indicators

- Transaction is unusual for the customer.
- Transaction is unusual for the country.
- Transaction is unusual for the industry.
- Transaction is unusual for any other reason.
- Transaction seems to be inconsistent with the customer's apparent financial standing or usual pattern of activities.
- Sudden unexplained increase in wealth.
- Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically advantageous for the customer.
- Transaction uses account(s) that have been dormant.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

Cash Transaction Indicators

- Customer suddenly starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past.
- Customer frequently exchanges small bills for large ones.
- Customer uses notes in denominations that are unusual for the customer, when the norm in that business is much smaller or much larger denominations.
- Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.
- Customer deposits musty or extremely dirty bills.
- Customer makes cash transactions of consistently rounded-off large amounts.
- Customer consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Customer consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Customer presents uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which could trigger reporting requirements.
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Customer frequently purchases traveler's checks, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the customer.
- Customer asks the Financial Institution to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.).
- Stated occupation of the customer is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area) .
- Customer consistently claims that source of funds is gambling winnings with no evidence of corresponding losses.

Indicators Involving Loans

- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.

- Loans that lack a legitimate business purpose; provide the bank with significant fees for assuming little or no risk; or tend to obscure the movement of funds (*e.g.*, loans made to a borrower and immediately sold to an entity related to the borrower).
- Customer claims true ownership of assets used for collateral, even though assets held in a different name.

Trade Financing Indicators

- Items shipped are inconsistent with the nature of the customer's business (*e.g.*, a steel company that starts dealing in paper products, or an information technology company that starts dealing in pharmaceuticals).
- Customers ship items through high-risk jurisdictions, including transit through countries recognized as non-compliant with AML/CFT requirements.
- Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions.
- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Transactions with Overseas or Offshore Jurisdictions

- Accumulation of large balances, inconsistent with the known turnover of the customer's business, and subsequent transfers to overseas or offshore account(s).
- Frequent requests for travelers checks, foreign currency drafts or other negotiable instruments.
- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-value deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transferred by customer to/from offshore jurisdictions on an in-and-out (pass through) basis.
- Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the customer's business or with national trade patterns.
- Use of a credit card issued by an offshore bank.

Suspicious Patterns involving Multiple Transactions

- Round trip transactions where funds are transferred to one destination, and then return in roughly the same amount from a different origin.
- Structured transactions that break transactions into smaller amounts to avoid reporting.
- Distributer/collector transactions where multiple accounts funnel into one, or one funnels into multiple without adequate explanation. This is an especially strong indicator when accounts may be controlled by single beneficial owner.

Transactions Involving Proxies

- Transactions where a person who is matched by two attributes (e.g. name and address, or name and birthday, or birthday and address) appears to maintain multiple accounts with variations in one of these parameters.
- Transactions with multiple accounts at the same address.
- Transactions where the address does not exist in public records.
- Transactions where the name does not exist in public records.
- Transactions where the account holder is a PEP.
- Transactions where the account holder is a relative or close associate of a PEP.
- Transactions where the account holder shares an address with a PEP.
- Large transactions by people with low-income jobs, especially when employed by or related to high wealth individuals.
- Transactions in the name of very young people.
- Transactions in the name of dead people.
- Transactions in the name of people living in areas where such wealth would be abnormal.

Red Flag Indicators for Specific Sectors

Securities Sectors

- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the client or their financial ability.
- Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed.
- Client attempts to purchase investments with cash.
- Client wishes to purchase a number of investments with money orders, traveller's cheques, cashier's cheques, bank drafts or other bank instruments, especially in amounts that are slightly less than the reporting threshold, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the client or their financial ability.

- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the client.
- Client frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the client.
- Several clients open accounts within a short period of time to trade the same stock.
- Client is an institutional trader that trades large blocks of junior or penny stock on behalf of an unidentified party.
- Unrelated clients redirect funds toward the same account.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transaction of very large value.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- All principals of client are located outside of Sri Lanka.
- Client attempts to purchase investments with instruments in the name of a third party.
- Payments made by way of third party cheques are payable to, or endorsed over to, the client.
- Transactions made by your employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which clients make settlements with cheques drawn by or remittances from, third parties.
- Unusually large amounts of securities or stock certificates in the names of individuals other than the client.
- Client maintains bank accounts and custodian or brokerage accounts at offshore banking centres with no explanation by client as to the purpose for such relationships.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money-laundering system.

Money/ Currency Changers

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Customer is reluctant to divulge the source of currency
- Customer is unable to produce relevant documents to support transaction
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
- Customer instructs that funds are to be picked up by a third party on behalf of the payee.

Mobile Money Service Providers

- Customer used multiple names/identities, in conjunction with providing multiple addresses, making it difficult to ascertain the true identity of the customer.
- The frequency of the customer's visits was excessive, and also involved the use a wide range of agent locations.
- The purpose of the transactions, and the relationship between the beneficiary and the ordering customer, does not appear to make business sense.
- Multiple senders transferring funds to a single individual
- Currency notes used are in “used notes” and/or small denominations (“used notes” may imply that notes are worn, dirty, stained, give off unusual smell, etc.)
- Customer attempts to send money to a person on a sanctions list
- Customer fails to provide verifiable identity information or refuses to provide verifiable identity information either for the customer and/or for the beneficiary
- Customer attempts to use or uses unusual or suspect identification documents.
- The customer wishes to engage in transactions that are inconsistent with the customer’s stated purposes when the account was initially set-up.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

@@23 @t.;,cJ C,ts)ts)a)
!BLDIJUJLWW L6TT6II!J3I◆!i:J ulrfl6lJ
FINANCIAL INTELLIGENCE UNIT

◆ (got») ®◆ @◆o◆E>
◆6\)f6161Dffi ID◆◆,IIJ 6lJ1'61ffil
CENTRALBANKOFSRILANKA

◆oC"> 30, d◆>IEJaffi ®le)o), ee>l◆® OJ, @ @otl'IIE)
®}6U. 30, 661ffildi)udi) L006l◆ 6il>◆, G&rr@tb4 - 01, ◆6Uffil6l>&
No. 30, Janadhlpathl Mawatha, Colombo 01, Sri Lanka

Circular No. 01/2022

Ref: 037/06/008/0006/020

January 10, 2022

To: CEOs / General Managers / Managing Directors of All Financial Institutions

Dear Sir/Madam,

Amendment to the Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021

Further to the Guidelines issued dated July 20, 2021, on the above.

Clause 15 of the above guidelines is amended as below.

15. Fis should maintain all infonnation captured in the CCTV system for a minimum period of 90 days.

Yours faithfully,

D R Karunaratne
Director/ Financial Intelligence Unit

Cc;

1. Director, Bank Supervision Department of the Central Bank of Sri Lanka
2. Director, Department of Supervision of Non - Bank Financial Institutions of the Central Bank of Sri Lanka
3. Director General, Securities and Exchange Commission of Sri Lanka
4. Compliance Officers, all Financial Institutions

ir 011-2477125
011-2477509
011-2477692
011-2477708
◆ flu@cbsl.lk
dflu@cbsl.lk
◆ www.flusrllanka.gov.lk

@@ot})J ®m @r;o<c>
CENTRALBANKOFSRILANKA
@@i:s §w c,Ci)
[61wlw6i) L6TT6l.l'6J ulrft61J
FINANCIAL INTELLIGENCE UNIT
l'.l'oCl 30, des>)WGffi ®)E)Cl), ®l® 01, @ @oQ)JE)
.@)GU. 30, U6Ul!T LI LDIT6U6il), GffirT@IDLI - 01, .@j6'1)6il)ffi
No. 30, Janadhlpathl Mawatha, Colombo 01, Sri Lanka

Guidelines No.02/2021

Ref: 03 7/06/008/0006/020

July 20, 2021

To: CEOs / General Managers/ Managing Directors of All Financial Institutions

Dear Madam/Sir,

Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 06 of2006 and the Financial Institutions (Customer Due Diligence) Rules, No. OJ of 2016.

YOURS faithfully,

E H Mohotty
Director/ Financial Intelligence Unit

Cc;

1. **Director, Bank Supervision Department of the Central Bank of Sri Lanka**
2. **Director, Department of Supervision of Non - Bank Financial Institutions of the Central Bank of Sri Lanka**
3. **Director General, Securities and Exchange Commission of Sri Lanka**
4. **Compliance Officers, all Financial Institutions**

011-241112s
011-2477509
011-2477692
011-2477708

flu@cbsl.lk dflu@cbsl.lk

www.tlusrllanka.gov.lk

Guidelines for FinancialInstitutions on CCTV operations for AML/CFT purposes, No. 2 of 2021

PARTI

Introduction

1. These Guidelines are issued pursuant to section 15(1)U) of the tfinancial Transactions Reporting Act, No. 06 of 2006 (hereinafter refe1Ted to as tfTRA).

2. These Guidelines are applicable to tfinancial Institutions (hereinafter referred to as tfis) that are engaged in or carrying out "finance business" as defined in Section 33 of the FTRA where closed-circuit television (hereinafter refe1Ted to as CCTV) systems are being used where relevant.

3. These Guidelines should be read along with the tfinancial Institutions (Customer Due Diligence) Rules, No. 0 I of 2016, issued by Gazette Extraordinary No. 1951/13, dated January 27, 2016 (hereinafter referred to as COD Rules). More specifically, these Guidelines should be referred together with Rules 7 and 11 of the COD Rules, to take measures specified therein for the purpose of having proper risk control and mitigation measures by having internal policies, controls and procedures to manage and mitigate money laundering and tel'orist financing risks and affiliating and integrating tfinancial Institution's money laundering and te1rnrist financing risk management with the overall risk management relating to the tfinancial Institution.

4. These Guidelines are issued in addition to the operational directives or circulars that are issued by the respective sector regulators with regard to CCTV systems.

5. These Guidelines are not intended to be exhaustive and do not constitute legal advice from the Financial Intelligence Unit. Nothing in these Guidelines should be construed as relieving tfis from any of their obligations under the tfTRA and regulations and rules issued thereunder.

Part II

The Requirements for CCTV Systems

6. As pat1 of the constant commitment to enhance operational risk management and safeguard banking operations against risks of being abused for money laundering and financing of terrorism, every FI is advised to have in place a robust CCTV system installed fully operational both within and outside of the premises. The business premises refer to the 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 (hereinafter referred to as CDD) is conducted.

7. In ensuring the CCTV system installed is effective to enable proper surveillance and monitoring of the business operations, all Fis should consider setting up a system of necessary standard with proper processes and controls, which could, at a minimum, cover the requirements set in in these Guidelines.

Placement ofCCTV cameras

8. In order to enhance the effective usage of the CCTV system, FIs need to ensure that CCTV cameras are installed at appropriate locations, in a manner that the camera is able to clearly capture, monitor and record the relevant areas where business operations take place. These locations are required to include the counters, customer interaction areas where CDD takes place, areas where safe deposit boxes are located, safe or vault and other cash handling areas, ATMs/CDMs, vehicle parking areas, the entrance and exit of the business premises, any other suitable areas, both inside and outside the building as detennined by the FI.

9. The CCTV surveillance systems must be aligned in a suitable manner and at an angle as to obtain a complete and unimpeded view of the area. Further, CCTVs need to be positioned in a manner where the capturing and processing inf01mation of the CCTV system is not interfered or impeded by internal or external lighting, glare, or any object.

Functions of CCTV system

I 0. Fis should ensure all images captured and recorded by the CCTV cameras are visible, recognizable and clear. The visual images or videos rendered through the CCTV cameras need to have the capability of identifying the features of the individuals, if any, that transact and should be clearly discernible from one image f'om another. In addition, adequate lighting must be maintained in order to capture clear CCTV footage.

11. Higher quality digital equipment should be used in CCTV systems to capture a clear frontal images of individuals. The CCTV systems should pennit easy viewing, recording and retrieval

of high-quality images (e.g., adequate number of pixels for improved zoom capabilities) of all information contained in CCTV system. Necessary technical specifications (e.g., resolution, frame rate) need to be maintained at a standard level to achieve an effective CCTV surveillance.

12. The CCTV systems of ATMs/CRMs/CDMs should remain operational throughout the 24-hours of a day - every day of the year, including during times when the FI is cJosed for business.

Real time monitoring

13. Fis should ensure real-time monitoring at the head office and/or branches or at a central monitoring unit, as far as practicable.

14. Fis are advised to obtain assistance of its security services personnel or law enforcement agencies (LEAs) to mitigate immediate risks that may arise to the FI's premises or to equipment, to its customers or to potential customers, or to any person at the vicinity of the CCTV camera, if such risk is detected based on CCTV footage obtained on real-time basis.

Maintenance of records

15. Fis should maintain all infom1ation captured in the CCTV system for a minimum period of 180 days.

16. Fis, at their discretion, may retain the CCTV recordings relevant to observed suspicious activities for a longer period.

17. The FIU, LEAs or any other competent authority would, fom time to time, instruct the Fls to retain the CCTV recordings relevant to a Suspicious Transactions Report furnished to FIU or any other related CCTV footage of a possible offending until the relevant investigations are concluded by the LEAs or other relevant competent authorities.

18. The Fis should ensure that its CCTV system(s) are capable of transfen-ing the info1mation to data storage devices, to allow retrieving and viewing of the CCTV records on electronic apparatus, such as computers.

19. To confirm the credibility of the CCTV records, Fis should ensure the timing of CCTV recording is properly set, synchronized and is consistent with the time and date of the operations that takes place at the business premises.

System administration and maintenance

20. FIs are expected to allocate adequate resources for CCTV monitoring systems, and sufficiently train the authorized personnel and staff to operate the CCTV system.

21. In order to asce11ain effective surveillance and monitoring of business operations, FIs should ensure that the CCTV system(s) deployed is/are properly maintained and operational, and remain under good working condition at all times.

22. The CCTV system should be equipped with the relevant features and functions to enable to implement control measures that will prevent such system f'om being manipulated or misused by any unauthorized parties.

23. Fis need to ensure that all inf01mation and records of the CCTV systems maintained safely and securely without unauthorized access and adequate controls are in place to prevent unauthorized alterations of records and access by unauthorized parties, by designating and appointing officers with appropriate responsibility and authorization levels, limiting system access only to relevant personnel to ensure proper accountability for the assigned functions.

24. Fis are expected to have procedures and mechanisms to ensure that regulators, LEAs and the FIU are able to obtain information and records in relation to money laundering investigations and prosecution upon request without delay.

25. FIs are required to issue internal operational guidelines on placement, functionality, monitoring, record keeping, system maintenance and administration, and include it as a pa11 of AML/CFT policy as well with the approval of BOD.

26. Procedures should be in place for periodical review and audit of the CCTV system(s) for number of existing cameras in the premises at branch level and where standalone ATM/CDM are located. Audits and reviews should ensure the adequacy of the number of cameras, functionality, accuracy, operability, record keeping and other salient requirements. A report of such review/ audit on the adequacy of CCTV coverage should be submitted to the Board of Directors (BOD) and to the senior management.

27. Based on the repo1t submitted to the BOD, if the quality and coverage of CCTV systems are inadequate or more quality and coverage is desired, the senior management and the BOD are advised to take appropriate steps to rectify such deficiency or increase the coverage as appropriate. Fmther, immediate steps should be taken to replace or upgrade the equipment soon after any malfunction is detected.

28. Fis should ensure activities relating to the maintenance and recalibration of the CCTV system including system upgrading, refo1111atting and removal of records are clearly recorded in the system's maintenance log and reported to the senior management, as appropriate.

ශ්‍රී ලංකා මහ බැංකුව

CENTRAL BANK OF SRILANKA

මූල්‍ය බුද්ධි ඒකකය நிதியியல் உளவறிதற் பிரிவு **FInanclal Intelligence Unit**

Ref: 037/07/006/0004/018

GuideWnes-04/2018

19 April 2018

To: CEO's of All Financial Institutions

Dear Sir / Madam

Guidelines on Identification of Beneficial Ownership
for Financial Institutions, No. 04 of 2018

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 and the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016.

Yours faithfully

D M **Rupasinghe**
Director
Financial Intelligence Unit

Cc : Compliance Officer

14 වන මහල, අංක **30**, ජනාධිපති මාවත,
තැ. පෙ. **590**, කොළඹ **01**, ශ්‍රී ලංකාව

14 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை
த. பெ. இல. 590, கொழும்பு 01, இலங்கை

tenet ia , He. 30, Jana0tip&1 Moatha,
P. 0. Bar. 590, Colombo 01. Sri Wka.

94 11 2477125 / 509 94 11 2477692 fiu@cbsl.lk **www.fiusrilanka.gov.lk**

Guidelines for Financial Institutions on Identification of Beneficial Ownership, No. 04 of 2018

I. Introduction

1. This Guideline is issued pursuant to section 15(1)(j) of the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA).

2. The Financial Intelligence Unit of Sri Lanka (FIU), acting within the powers vested with it under the FTRA, issued the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 (CDD Rules) by Gazette Extraordinary No. 1951/13, dated January 27, 2016, effective from the date of issue, applicable to institutions that engage in "finance business" as defined under Section 33 of the FTRA.

3. Rules 28-31, 48-50 of the CDD Rules established, inter alia, provisions requiring Financial Institutions (FIs) identified under the Rules to take appropriate measures to identify and verify the natural person(s) who are the ultimate "beneficial owners" of a customer that is a legal person or legal arrangement, as defined in Rule 99 of the CDD Rules.

4. This Guideline is provided as an aid to interpret and apply CDD Rules. The Guideline is not intended to be exhaustive and it does not impose legally binding practices on any FIs, and it does not constitute legal advice from the FIU. Nothing in this Guideline should be construed as releasing FIs from any of their obligations under the CDD Rules or the FTRA.

II. Background/Context

Who is a beneficial owner?

5. As per the Rule 99 of the CDD Rules, 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. According to Rule 49, controlling ownership interest means an interest acquired by providing more than ten percent (10%) of the capital of a legal person.

6. It is an FI's obligation to determine the natural person(s) who is/are the ultimate beneficial owner(s). The ultimate beneficial owner 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.

7. 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 is acting on behalf of another or if another person is the beneficial owner of the property of the customer.

Why is it important to identify the beneficial owner?

8. Corporate entities such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements conduct a wide variety of commercial and entrepreneurial activities. However, despite the essential and legitimate role that corporate entities play in the economy, under certain conditions, they have been misused for illicit purposes, including money laundering (ML), bribery and corruption, insider dealings, tax fraud, terrorist financing (TF), and other unlawful activities. This is because, for criminals trying to circumvent anti-money laundering (AML) and countering the financing of terrorism (CFT) measures, corporate entities provide an attractive avenue to disguise the ownership and hide the illicit origin.

9. Various studies conducted by Financial Action Task Force (FATF), World Bank, United Nations Office on Drugs and Crime (UNODC) have explored the misuse of corporate entities for illicit purposes, including for ML/TF. In general, the lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising:
   a) the identity of known or suspected criminals,
   b) the true purpose of an account or property held by a corporate entities, and/or

c) the source or use of funds or property associated with a corporate entities.

Ways in which beneficial ownership information can be hidden/obscured

10. Beneficial ownership information can be obscured through various ways, including but not limited to;
    a) use of shell companies [1] (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions,
    b) complex ownership and control structures involving many layers of ownership, sometimes in the name of other legal persons and sometimes using a chain of ownership that is spread across several jurisdictions,
    c) bearer shares and bearer share warrants,
    d) use of legal persons as directors,
    e) formal nominee shareholders and directors where the identity of the nominator is undisclosed,
    f) informal nominee shareholders and directors, such as close associates and family,
    g) trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,
    h) use of intermediaries in forming legal persons, including professional intermediaries such as accountants, lawyers, notaries, trust and company service providers,

III. Establishing the Beneficial Owner

A) Beneficial owner of Legal Persons

11. As per Rule 99 of the CDD Rules, "legal person" means any entity other than a natural person that is able to establish a permanent customer relationship with a financial institution or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association.

[1] Shell companies are companies that are incorporated with no significant operations or related assets, including an absence of physical presence

12. In the process of identifying beneficial owner(s) of a legal person, FIs have to consider three main elements:

    a) Which natural person(s) owns or controls more than ten percent (10%) of the customer's equity?
    b) Which natural person(s) has "effective control" of the legal person?
    c) On behalf of which natural person(s) the transaction is being conducted?

13. The beneficial owner(s) of a customer (legal person) may satisfy one or more of the three elements identified above. Accordingly, it would not be sufficient to simply apply only the ownership element in determining beneficial ownership.

Ownership

14. 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

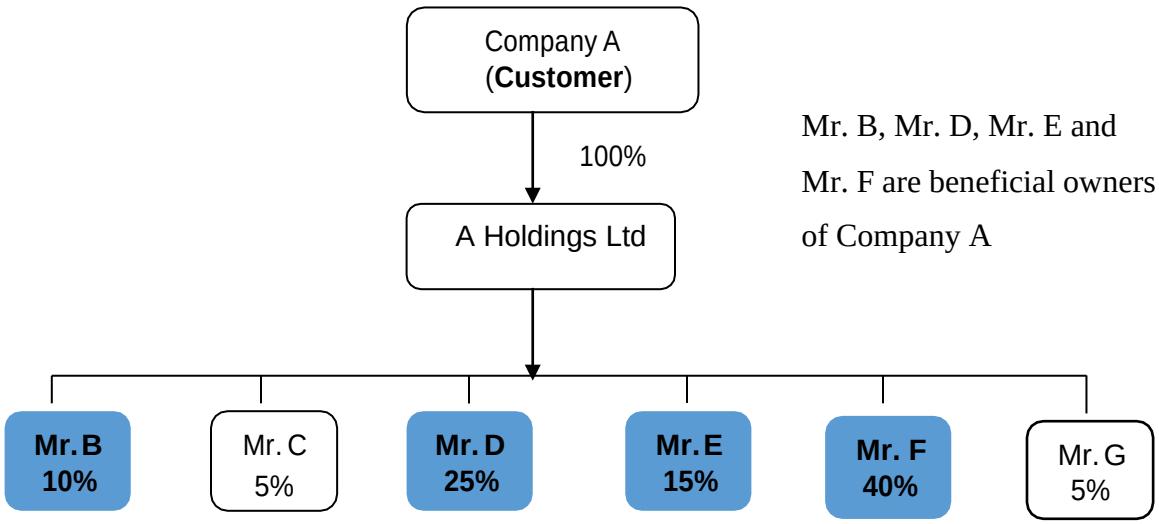
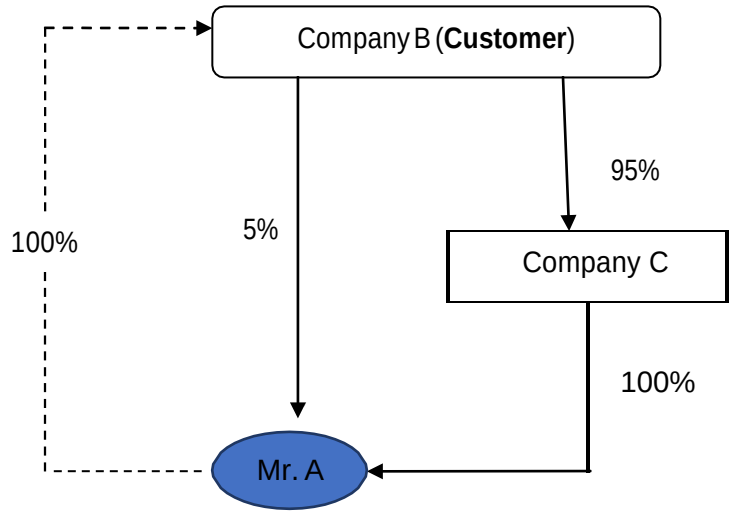
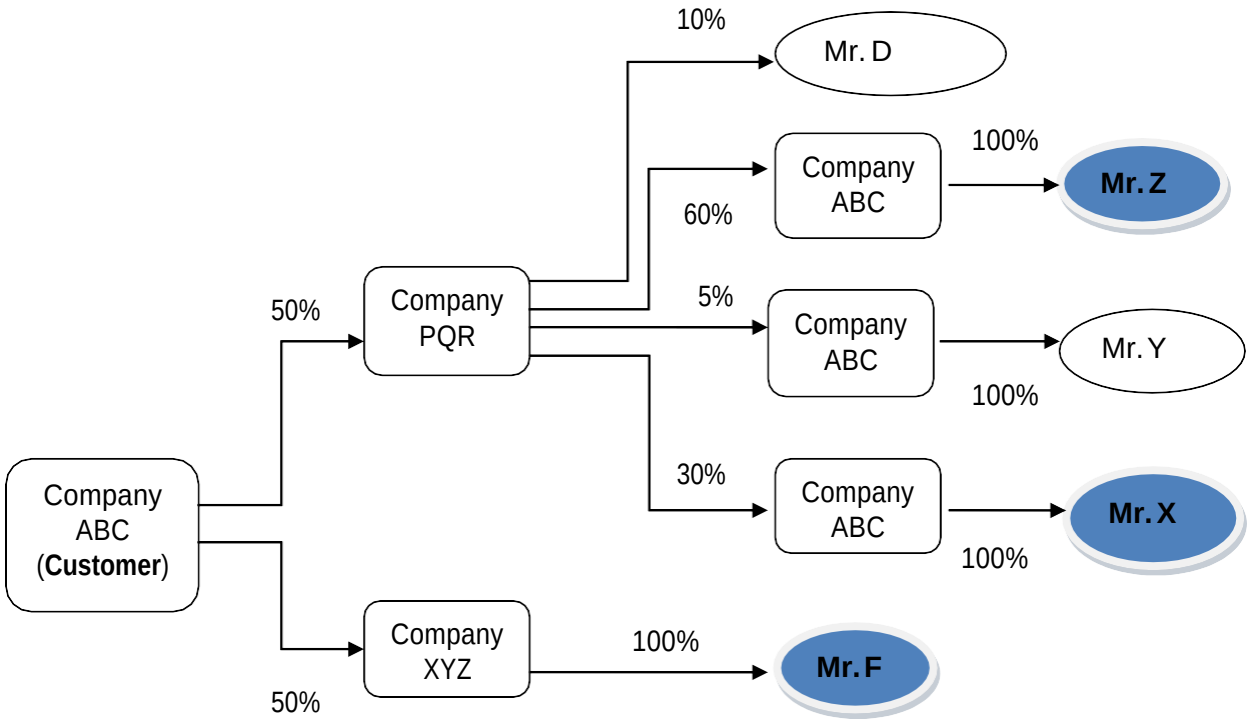


Figure 2: Direct and Indirect Share Holdings



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

15. A natural person that exercises control over a controlling portion of equity interest, either directly, via nominees or via family members or close associates (whether disclosed or undisclosed) who nominally own or control the shares, can be considered as a beneficial owner. A majority shareholder or a majority formed by some combination of shareholders that are nominees for a natural person is also a beneficial owner.

16. For some customers, ownership may be spread over a large number of individuals with all individual owning less than ten percent (10%). In such instance, because no individual(s) owns more than ten percent (10%), the effective control element outlined below would be more appropriate to determine the beneficial owner(s)/controller(s).

Effective Control

17. 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).

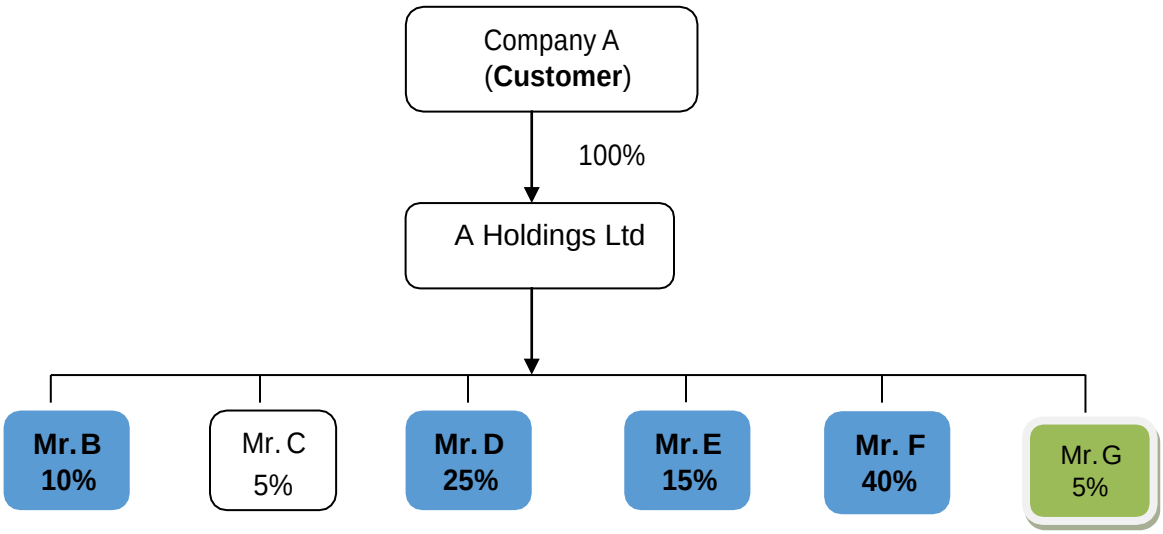
18. Natural persons may also control the legal person through other means such as:
    a) Personal connections to persons in positions such as Executive Directors/ CEOs/ Managing Director or that possess ownership;

b) Significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person;

c) Control without ownership by participating in the financing of the enterprise, or because of close family relationships, historical or contractual associations, or if a company defaults on certain payments;

d) Use, enjoyment or benefiting from the assets owned by the legal person even if control is never exercised.

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.

Person on whose behalf a transaction is being conducted

19. Another aspect of the definition of beneficial ownership is a person on whose behalf a transaction is conducted. This may be the individual who is an underlying client of the customer. An example is, if a FI knows that person 'A' is conducting an

occasional transaction on behalf of person ‘B’, and then person ‘A’ and person ‘B’ should be identified and verified along with any other beneficial owners that may be a party to transaction.

20. Acting on behalf of the customer is when a person is authorized to carry out transactions or other activities on behalf of the customer. However, ‘Authority to act’ should not be confused with effective control.

21. There are instances where persons are acting on behalf of a customer may not necessarily be the beneficial owners of that customer.

22. As per Rule 29, the FI has to identify the natural persons that act on behalf of the customer and verify the identity of such persons. The authority of such person to act on behalf of the customer also should be verified through documentary evidence including specimen signatures of the persons so authorized.

B) Beneficial owner of legal arrangements

23. As defined under Rule 99, legal arrangement includes an express trust, a fiduciary account or a nominee.

24. All trusts have the common characteristic of causing a separation between legal ownership and beneficial ownership. Legal ownership always rests with the trustee. Beneficial ownership can rest with the author of trust, trustees or beneficiaries, jointly or individually.

25. As per Rule 50, FIs should identify and take reasonable measures to verify information about a trust, including, 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).

26. FIs are required to obtain trust documents (e.g. deed of trust, instrument of trust, trust declaration, etc.) and the provisions of the trust document must be fully understood within the context of the laws of the governing jurisdiction. The FIs should take reasonable measures to verify trust document through independent means (e.g. Registry of Trust, Notary)

Example:

Person 'A' is the author of a trust for the benefit of his child. The trustee seeks to establish a relationship with a financial institution to help manage the assets of the trust. Even though the trustee is the controller of the assets of the trust he may not be the ultimate beneficial owner and the main focus of CDD should include person 'A'" as well.

IV. Identification and Verification of beneficial ownership information

27. As per Rule 30, FIs 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 FIs to satisfy itself that it knows who the beneficial owner(s) is.

28. Accordingly, the identification of beneficial owner is mandatory. Once the FI establishes who the beneficial owner(s) of a customer is/are, the FI 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.

29. As per Rule 31, FI is required to verify the identity of the beneficial owner before or during the course of entering into a business relationship with, or conducting a transaction for an occasional customer.

30. Accordingly, once the identity is established, the FIs have to take reasonable measures to verify the identity of the beneficial owner(s). The reasonable measures for verification should be determined subject to the risk and complexities of the ownership and control structure of the legal person or arrangement.

31. Simplified verification procedures can be applied for verification of beneficial ownership of legal persons that are already subject to rules regarding corporate governance and transparency such as those that apply to firms with shares that publicly trade on a well-regulated exchange, or with simple and locally-familiar ownership structures or legal persons who are expected to conduct low risk transactions.

32. For the verification of beneficial ownership, some of the documentation that FIs can rely on may include (but not limited to) the following:
    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.

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

34. As per Schedule I of the CDD Rules, 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, FIs can use relevant identification information available from reliable sources (e.g. a public register) to identify the Directors and major Shareholders.

35. As per Rule 49 (d), FIs have to identify the natural persons holding senior management positions as beneficial owners when FIs are unable to determine the beneficial owner as there is no person owning more than ten percent (10%) of the customer's equity or no individual exercising control over the customer.

Periodic Review of Information

36. As per Rule 40, FIs should periodically review the adequacy of information obtained in respect of beneficial owners to ensure that the information is up to date. The review period and procedures thereof should be decided by each FI in its internal AML/CFT Policy according to the risk-based approach.

37. Any material/significant change in customer circumstances may necessitate a review of beneficial ownership. Some examples of material/significant changes include:
    a. a public company is taken private;
    b. a shareholder or group of shareholders takes effective control of voting shares;
    c. a new partner is added, or an existing partner is removed;
    d. change in management positions;
    e. new trustees are appointed;
    f. a trust is dissolved;
    g. a new account is opened for the same customer;
    h. transactions are attempted that are inconsistent with the customer's profile.

Delayed Verification

38. As per Rules 31 and 32, FIs are allowed to delay the verification of identity of beneficial owners when,

a. risk level of the customer is low and verification is not possible at the point of entering into the business relationship,
b. there is no suspicion of money laundering or terrorist financing risk involved,
c. delay will not interrupt the normal conduct of business.

39. As per Rule 33, when delayed verification is allowed, FIs should adopt risk management procedures relating to the conditions under which the customer may utilize the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amounts of transactions that can be performed and the monitoring of large or complex transactions being carried outside the expected types of transactions for that relationship.

40. As per Rule 36, FIs should not establish a business relationship or conduct any transaction with a customer who poses a high money laundering and terrorist financing risk, prior to verifying the identity of the beneficial owner.

41. As per Rule 35, when an FI is unable to comply with CDD measures as required in CDD Rule including identification and verification of beneficial ownership information, the FI should not enter into the business relationship or perform the transaction with new customers and terminate the business relationship with existing customers and consider making a suspicious transaction report in relation to the customer.

V. Other Requirements

Declaration of beneficial ownership by the customer

42. FIs may obtain beneficial ownership information either by obtaining the required information on a standard certification form (Certification Form (Appendix A) or by any other means, up to the satisfaction of the FIs with regard to the identification of the beneficial owner(s).

43. Use of the form is optional and FI may substitute this form with a version that is suitable, whether paper or electronic, so long as the required information is collected, protected, preserved and made available to competent authorities upon demand and records are maintained in accordance with the CDD Rules and FTRA.

44. FIs are required to document the procedure to be followed in the identification and verification of beneficial ownership requirements relating to legal persons and arrangements in the AML/CFT Policy approved by the Board of Directors.

Record Keeping Obligations

45. The FIs are required to maintain records of identification and verification information relating to beneficial ownership as prescribed under Part V of the CDD Rules and FTRA.

Beneficial owners who are Politically Exposed Persons (PEPs)

46. As per Rule 59, FIs are required to implement appropriate internal policies, procedures and controls to determine if the beneficial owner is a politically exposed person. Through such process if the FI identifies any beneficial owner as a PEP, the relationship should be considered as high risk and subject to enhanced due diligence as required in the CDD Rules.

Sanctions

47. Failure to comply with the beneficial ownership requirements as required under the CDD Rule will be a violation of the Section 2 (3) of the FTRA and will be punishable under Section 19 of FTRA.

VI. Examples

Example 1: Record for ownership and control structure of a legal person

ABC Company Ltd. is a private limited liability company registered under the Companies Act, No. 7 of 2007. Mr. A owns 25% of the shares and BC Company Ltd. owns the balance 75% of shares of ABC. Mr. S is Managing Director of ABC

Company and; the Board of Directors consists with his wife, Mrs. S, ABC's Chief Financial Officer; and their three children.

In this example, FIs required to record:

- the ownership of the Company - shared by Mr. A (25% of the shares) and BC Company Ltd. (75% of the shares);
- the ownership structure of the entity - ABC Company Ltd. is a privately traded.
- the identification of all members the Board of Directors (Mr. S's Family) as they are having effective control;
- Identification of Mr. A as he is having more than 10% of ownership
- identification of all of the individuals who own or control, directly or indirectly, 10% or more of the shares of BC Company Ltd since it owns 75% of the shares, it also exercises control. However, in a case like this, FI must research further to determine whether any individual owns enough shares of BC Company Ltd. that would constitute 10% of ABC Company Ltd., or until FI determine that there is no such individual;
- the manner in which FI obtained this information; and
- the measures taken to verify accuracy of information.

Example 2
Record for ownership and control structure of partnership

Rainbow Property Developers is a partnership engaged in buying and selling of real estate in Western Province owned by two partners (Mr. T and Mr. J). Mr. T and Mr. J have signed a partnership agreement stating that Mr. T will invest Rs. 5,000,000 in the partnership to rent space for the Rainbow Property Developers and other administrative expenses, and Mr. J will be solely responsible for operations of the business. All decisions related to the partnership must be unanimous; in case of a disagreement, either partner can decide to end the partnership. Mr. T & Mr. J will split the profits from the business 50/50. If they decide to end the partnership, Mr. T

will get 55% of the proceeds of the sale of the business assets, while Mr. J will get 45%.

In this example FI, is required to record:

- the ownership structure of the entity, including the details of the partnership between Mr. T & Mr. J;
- identification of Mr. T and Mr. J as both control the partnership;
- the manner in which, the FI obtained this information; and
- the measures taken to confirm accuracy of information.

Note: The business structure is important in this example as the ownership and control of the partnership is shared between Mr. T & Mr. J. The FI needs to retain a copy of the partnership agreement to meet record keeping requirements as well as confirm the accuracy of the beneficial ownership information obtained. In the absence of such agreement it should be recorded that the partnership exists between Mr. T and Mr. J without having a written agreement.

Issued on April 19, 2018

APPENDIX I—Beneficial Ownership Form

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* 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 : (By signing you attest to the veracity of all information contained herein and you acknowledge and understand the above warning)

Verification of Beneficial Ownership

Authorized Financial Institution 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

A LIST CATEGORIES OF CUSTOMERS THAT CAN BE CONSIDERED AS PEPS

DOMESTIC PEPS

A.

1 The President
2 The Prime Minister
3 The Speaker and the Deputy Speaker of the Parliament
4 Cabinet Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers
5 Members of Parliament
6 Leaders of Political Parties

B.

7 Governors of Provinces
8 Chief Ministers of Provinces
9 Mayor, Chairman of Municipal Councils
10 Chairman of Provincial Councils
11 Members of Municipal Councils/ Provincial Councils / Local Government Bodies
12 Commissioners/ Secretaries to Municipal Councils/ Provincial Councils / Local Government Bodies

C.

13 Chief Justice
14 Attorney General
15 Judges of Supreme Court
16 Judges of the Court of Appeal
17 Solicitor General of the Attorney General's Department
18 Judges of High Courts/Provincial High Courts
19 Judges of District Courts
20 Judges of Magistrate Courts
21 Registrar of Supreme Court
22 Registrar of the Court of Appeal
23 Registrars of Judges of High Courts/Provincial High Courts
24 Registrars of District Courts
25 Registrars of Magistrate Courts

D.

26 Ambassadors /High Commissioners
27 Consul-General/ Deputy Head of Mission/Charge d'affaires/Honorary Consul
28 Ministers plenipotentiary and Envoys Extraordinary
29 Representatives of UN agencies and Heads of other international organizations

E.

30 Secretary/ Senior Additional Secretaries/ Additional Secretaries to the President
31 Secretary/ Senior Additional Secretaries/ Additional Secretaries to the Prime Minister

32 Secretary /Senior Additional Secretaries/ Additional Secretaries to the Cabinet of Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers
33 Deputy Secretary to the Treasury
34 Secretary/ Senior Additional Secretaries /Additional Secretaries/ Deputy Secretaries to Ministries
35 Members of the Monetary Board
36 Governor / Deputy Governors / Assistant Governors and Heads and Additional Heads of Department of the Central Bank of Sri Lanka
37 Advisors to the President/ Prime Minister / Ministers/ Ministries
38 Chief of staff of presidential secretariat
39 Auditor General
40 Secretary General of Parliament
41 District Secretaries/ Government Agent and Secretaries
42 Heads and Senior Officials of Government Departments
43 Chairmen and Senior Officials of State Enterprises
44 Chairmen and Senior Officials of State Corporations / Statutory Boards/ Authorities/ Public Corporations

F.

45 Field Marshall / Admiral of the Fleet/ Marshal of the Air Force
46 Chief of Defence Staff
47 General of Sri Lanka Army/Admiral of Sri Lanka Navy/ Air Chief Marshal of Sri Lanka Air Force
48 Officers in the Rank of Lieutenant Colonel and above of Sri Lanka Army
49 Officers in the Rank of Commander and above of Sri Lanka Navy
50 Officers in the Rank of Wing Commander and above of Sri Lanka Air Force
51 Inspector General of Police
52 Police officers above the rank of Asst. Superintendent of Police

G.

53 Chairman/ members and senior officers of the Public Service Commission
54 Chairman/ members and senior officers of the National Police Commission
55 Chairman/ members and senior officers of the Human Right Commission
56 Chairman/ members and senior officers of the Commission to Investigation Allegations of Bribery or Corruption
57 Chairman/ members and senior officers of the Finance Commission
58 Chairman/ members and senior officers of the Election Commission
59 Members of Constitutional Council
60 Chairman/ members and senior officers of the Audi Service Commission
61 Chairman/ members and senior officers of the Delimitation Commission
62 Chairman/ members and senior officers of the National Procurement Commission
63 Members of Cabinet appointed committees

H.

64 Chairman, Members and senior officers of University Grant Commission
65 Chairman, members of University Councils
66 Chancellor
67 Vice Chancellor
68 Registrar of universities

FOREIGN PEPS

69 Officials of international organizations who hold or have held, in the course of the last 5 years, management positions in such organizations (directors, heads of the boards or their deputies)
70 Officials of international organization who perform or performed any other management functions on the highest level, particularly in international and intergovernmental organizations,
71 Members of international parliamentary assemblies,
72 Judges and management officials of international courts

A LIST OF RED FLAGS AND INDICATORS FOR SUSPICION

A. PEPs attempting to shield their identity:

1. Use of corporate vehicles (legal entities and legal arrangements) to obscure
    i) ownership,
    ii) involved industries or
    iii) countries.
2. Use of corporate vehicles without valid business reason.
3. Use of intermediaries when this does not match with normal business practices or when this seems to be used to shield identity of PEP.
4. Use of family members or close associates as legal owner.

B. Red flags and indicators relating to the PEP and his behavior

1. The PEP makes inquiries about the institution's AML policy or PEP policy.
2. The PEP seems generally uncomfortable to provide information about source of wealth or source of funds.
3. The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries.
4. The PEP is unable or reluctant to explain the reason for doing business in the country of the FIs/DNFBs.
5. The PEP provides inaccurate or incomplete information.
6. The PEPs seeks to make use of the services of a FIs/ DNFBs that would normally not cater to foreign or high value clients.
7. Funds are repeatedly moved to and from countries to which the PEPs does not seem to have ties with.
8. The PEP is or has been denied entry to the country (visa denial).
9. The PEP is from a country that prohibits or restricts its/certain citizens to hold accounts or own
   certain property in a foreign country.

C. PEP's position or involvement in businesses:

1. The PEP has a substantial authority over or access to state assets and funds, policies and operations.
2. The PEP has control over regulatory approvals, including awarding licences and concessions.
3. The PEP has the formal or informal ability to control mechanisms established to prevent and detected ML/TF.
4. The PEP (actively) downplays importance of his/her public function, or the public function he is relates to associated with.
5. The PEP does not reveal all positions (including those that are *ex officio*).
6. The PEP has access to, control or influence over, government or corporate accounts.
7. The PEP (partially) owns or controls FIs/ DNFBs, either privately, or *ex officio*.
8. The PEP (partially) owns or controls the FIs/ DNFBP (either privately or *ex officio*) that is a counter part or a correspondent in a transaction.
9. The PEP is a director or beneficial owner of a legal entity that is a client of a FIs/DNFB.

D. Red flags and indicators relating to the industry/sector with which the PEP is involved:

1. Arms trade and Defence industry.
2. Banking and finance.
3. Businesses active in government procurement, *i.e.*, those whose business is selling to government or state agencies.
4. Construction and (large) infrastructure.
5. Development and other types of assistance.
6. Human health activities.
7. Privatization.
8. Provision of public goods, utilities.

RED FLAGS ON INFORMAL VALUE TRANSFER SYSTEMS

Money or Value Transfer Services perform an important role in the economy and the financial sector of a country. Money or Value Transfer Services can be classified into two types as Formal and Informal Money or Value Transfer Services based on the functional formality and characteristics. Formal Money or Value Transfer Services are expected to capture all economic transactions that add value to the national output of the country. However, Informal Money or Value Transfer Services (IMVTS) pose a significant threat to a nation's economy since the value created through IMVTS is not considered when assessing the national output. Furthermore, IMVTS could be abused for Money Laundering/Terrorist Financing (ML/TF) and related unlawful activities.

IMVTS mainly involve four parties and two geographical locations, i.e., sender, receiver and two IMVTS operators. In IMVTS, money is given by the sender in the first geographical location to an IMVTS operator of that location, to transfer the money to the receiver in the second geographical location, with the support of an IMVTS operator in the second location, preferably to settle payables. Above transactions are carried out with the use of the two currencies of the respective locations and it should be noted that no inward/outward remittances occur between the said locations.

Accordingly, the Financial Intelligence Unit (FIU) wishes to share the following list, that includes several red flag indicators observed by the FIU when carrying out analysis on Suspicious Transactions Reports received pertaining to IMVTS.

1. Receipt of foreign remittances to accounts initially and its gradual decrease/cessation followed by the receipt of Sri Lankan Rupees
   (This could be an indication that the accountholder(s) has shifted from formal money transfers systems to IMVTS)
2. Receipt of frequent third-party deposits and transfer of those funds to multiple third-party accounts
   (This could be an indication that the accountholder(s) is involved in IMVTS)

3. Minimal / no ATM withdrawals but substantial number of online debit fund transfers from accounts with names of receivers as narrations
   (This could be an indication that funds received to the country through IMVTS are distributed to the beneficiaries)
4. Receipt of frequent third-party deposits and withdrawal of such funds from abroad
   (This could be an instance where IMVTS intersect formal value transfer systems)
5. Accounts having an insignificant daily balance but an unusually high credit and debit turnover
   (This could be an indication that accounts are solely used for the purpose of distributing funds received through IMVTS)
6. Upon inquiries made by the reporting entity, accountholders themselves declaring to be engaged in IMVTS operations

The financial institutions are hereby required to take cognizance of the above red flags/ risk indicators and take appropriate actions to reduce the possible ML/TF risk, if any, arising from these transactions, including considering escalating the indicators to the level of raising STRs with the FIU.

Red Flag Indicators - 04/2021

Trend in Foreign Currency Outflows via ATMs: Cash withdrawals in the United Arab Emirates (UAE)

The Financial Intelligence Unit (FIU) has observed significant number of transactions where foreign currency withdrawals from the UAE are reported using locally issued ATM cards.

It was noticed that some individuals collect deposits to the individual accounts from several areas of Sri Lanka and the accumulated funds in these accounts have been withdrawn almost immediately, via ATMs in the UAE**.**

FIU observed the following common characteristics when analyzing the patterns of the transactions:

1. Often, the majority of the accounts have been opened recently (in 2021).
2. Rupee value of most of the cash withdrawals from ATMs in the UAE is around Rs.100,000 to 200,000 per withdrawal. Occasionally, several such withdrawals had been taken place on the same day.
3. A significant number of suspected accounts have been opened at bank branches located in areas such as Kandy, Kalmunai, Wellampitiya, Kanthale and Colombo.
4. The ATM withdrawals were made from the UAE within 2 – 3 days after the opening of those reported accounts.
5. Cash has been withdrawn using several ATM cards at the same location at the same time, suggesting a single user having multiple cards or a group of persons acting in concert.

These activities suggest that the transactions may be linked to:

a. money laundering or terrorist financing activities
b. trade related activities, where ATM cards issued by banks are being misused for bulk withdrawals in foreign jurisdictions; or
c. activities linked to transfer funds without declaration at the border – suspicion is linked to tax evasion, or informal money, or value transmitters' (hawala or hundi) outflows.

The financial institutions are required to take appropriate actions to reduce the possible ML/TF risk, if any, arising from these transactions. Particular attention has to be drawn to:

I. Possible foreign exchange violations
II. The account holders allowing third parties to use their debit cards for cash withdrawals in foreign countries
III. Ongoing monitoring of customers after establishing the business relationship should be strengthened
IV. Necessary actions should be initiated, if the account holders are not reachable through the given contact numbers
V. If there is any suspicion, it has to be reported to the FIU under section 7 of the FTRA

l@ot»l ®m @t;o c>
8)60r616Ulffi lD��lU6lJr:ilffil
CENTRALBANKOFSRILANKA

i@?S���Q)Q
[6l�wlUJoo �61l6l.J�l'f>!D t.'.irft&lf
FINANCIAL INTELLIGENCE UNIT

t,ot»30,�ijeo,®lt>a>,�J�®01,@@otme>
�6\). 30, cf60TIT,U{bl l.OfT6l.J$l)6l»�, G6>fT@LD4 - 01, �6\)ffiJ6IDffi
No. 30, Janadhlpathl Mawatha, Colombo 01, Sri Lanka

Guidelines-03/2020

Ref: 037/05/006/0009/020

October 22, 2020

To: CEOs / General Managers and Managing Directors of All Financial Institutions

Dear Sir/ Madam,

Guidelines for Non Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No. 3 of 2020

The above mentioned Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) and Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 (CDD Rules) as amended from time to time.

Yours faithfully,

Director
Financial Intelligence Unit

Cc;

1. Director, Bank Supervision Department of Central Bank of Sri Lanka
2. Director, Department of Supervision of Non-Bank Financial Institutions of Central Bank of Sri Lanka
3. Director, Payments and Settlements Department of Central Bank of Sri Lanka
4. Director General, Securities and Exchange Commission of Sri Lanka
5. Director General, Insurance Regulatory Commission of Sri Lanka
6. Commissioner General, Department for Registration of Persons
7. Compliance Officers, all Financial Institutions

tr 011-2477125 alt 011-2477692 flu@cbsl.lk www.flusrllank.gov.lk
011-2477509 011-2477708 dflu@cbsl.lk

E H Mohotty

Guidelines for Non Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No. 3 of 2020

Part I - Introduction

1. These Guidelines are issued pursuant to section 15(1) (j) of the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA).

2. These Guidelines are issued to Financial Institutions (FIs) to facilitate verification of identity (verification against the original document) when onboarding non face-to-face[1] individual customers (natural persons) using electronic interface provided by the Department for Registration of Persons (hereinafter referred to as DRP).

3. These Guidelines will come into force with immediate effect and shall be read together with the FTRA and Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 (CDD Rules) as amended from time to time.

4. These Guidelines may be modified from time to time or withdrawn in the event of any unforeseen risks arising in the future or when more effective and reliable methods for establishing and verifying customer identity in non face-to-face onboarding come into force.

Part II - Scope

5. These Guidelines provide alternate methods to meet the requirement of "verification against original document" for individual customers who are natural persons as detailed in the following:

    a) Schedule to the CDD Rules under Rule 27 – Item (1) (b)(i)—verification of identity document
    b) Schedule to the CDD Rules under Rule 27 – Item (1) (b)(ii)—verification ofaddress

6. All other requirements imposed under CDD Rules will be applicable to customers onboarded using the above method without any exception.

Part III - Methods of Application

7. Verification of individual customer identity document

    a. Claimed Identity. FIs must continue to identify their customers in full accordance with CDD Rule 27(1)(a) and obtain all information described in Rule 27(1)(b) from the customer.

        Claimed identity information may be obtained by the FI in any manner that safeguards its integrity during the process of transmission. Potential modes of obtaining identity

[1] **Non-face-to-face** interactions are considered to occur remotely, meaning the parties are not in the same physical location and conduct activities by digital or other non-physically-present.

information include but are not limited to electronic forms, mobile app, video conferencing, secure email, kiosks/ ATMs/ CDMs, registered post, etc.

Use of agents, third-party service providers acting as agents or reliance on third-party FIs or designated non-finance businesses to collect information on claimed identity is not permitted for this alternate method.

b. Existence of Claimed Identity. FIs may use electronic interface published by the DRP to obtain information to independently validate the customer's claimed identity, provided:

   i. The interface is accessed with the unique credentials assigned to the FI by the DRP;
   ii. The interface is accessed strictly in accordance with its terms of use;
   iii. The interface returns to the FI a record that uniquely matches the claimed identity information provided by the customer in a form suitable for verification of customer identity claims and that includes an image of the person to which the identity has been assigned that is suitable for the purpose of associating the record with the claimed identity of the customer;
   iv. The FI has no reason to believe that the interface, or the effectiveness thereof, has been maliciously compromised in any way.

c. Associating Claimed Identity with Customer. The following steps must be performed in order to associate the claimed identity with the customer:

   i. Obtaining Customer Imagery and other documents from the Customer:
   High-quality still images[2] of the customer, ID documents and address verification documents must be obtained. For customers not physically present in Sri Lanka, passport images must also be obtained containing customer biographical data, a current visa and an entry stamp or any other entry permitting official document for the country where they are located. The imagery should be of sufficient quality to read details and to inspect security features of the identity document, to identify unique facial features of the customer, and to detect any potential alterations to the document. Ideally, the imagery should be obtained from a device known to be associated with the customer (e.g. a mobile phone) or from a dedicated device operated by, or on behalf of, the FI (e.g. kiosk devices).

   ii. Obtaining Customer Real-Time Video from the Customer
   A staff member of the FI must engage in a high-quality real-time video[3] conference with the customer and verify the possession of his identity documents and address verification documents during this real-time video conference. For customers not physically located in Sri Lanka, passport and visa data from (i) must also be verified. The customer should respond via real-time video conference to FI inquiries in order to establish the authenticity of the imagery and the accuracy of other customer provided information.

[2] High-quality still images refer to resolution equivalent to 300 PPI/ DPI (Pixels Per Inch / Dots Per Inch) or higher.
[3] High-quality real-time video refers to consistent resolution equivalent to 360p (pixels) or higher with minimal frame droppage.

iii. Obtaining Customer Imagery from DRP

FIs must use electronic interface published by DRP in order to obtain information to authenticate the validated identity information against the customer claimed identity, in accordance with the provisions detailed in paragraph 7(b). As a practical matter, the only currently available information for this purpose is a photographic image associated with a National Identity Card (NIC).

iv. Authenticating Claimed Identity to Customer

The following modes shall be used to authenticate the claimed Identity to the Customer:

1. Algorithmically: FIs that intend to authenticate a claimed identity algorithmically using data and images obtained from both the customer and DRP must obtain prior approval from the FIU in the form of an "enforcement forbearance" by submitting an application to the CBSL "Regulatory Sandbox" and completing the FIU's addendum to the application. Without such a forbearance and FI agreement with the FIU to abide by the terms of the forbearance, FIs are not permitted to authenticate claimed identities using this mode.

   The Sandbox Framework documents along with the Sandbox application form can be downloaded at https://www.cbsl.gov.lk/en/public-notices. For any inquiries or clarification contact Payments and Settlements Department of Central Bank of Sri Lanka on 2477542, 2477642 or e-mail to sandbox@cbsl.lk.

2. Manually: Manual comparison by employees of the FI should be made in all cases when an algorithmic comparison has not been approved by the FIU through guidelines or specific letters of forbearance [e.g. obtained through the CBSL Regulatory Sandbox]. The standard for successful non face-to-face authentication should be at least as rigorous as for the FI's face-to-face mode.

3. A combination of algorithmic and manual modes may also be used. However, if the algorithmic mode employed has not been approved by the FIU through guidelines or specific letters of forbearances then the manual mode must stand-alone as being determinative.

When the claimed identity cannot be verified or authenticated the FI must not enter into a business relationship with the customer or process transactions on behalf of the customer using this alternative verification method.

8. Verification of Individual Customer Address

Individual Customer addresses may be verified using data matching the customer's claimed identity obtained by the FI through a DRP electronic interface. If the address provided by the customer differs from the address obtained through a DRP electronic interface, the FI must instead verify the customer's address using independent data or services provided electronically to the FI directly from one or more sources specified in Schedule to the CDD Rules under Rule 27- Item (1)(a)(a1)(iii).

9. Instances where FIs should refrain from opening accounts or establishing business relationships non face-to-face.

    a. When non face-to-face customer uses any other identification document other than national identity card such as passport or driver's license to identify himself.

    b. When high quality interactive real time video of the customer cannot be obtained.

    c. When high quality data and still images of customer identity documents cannot be obtained.

    d. When identity documents presented by the customer appear damaged or degraded to the point that they are no longer fit for the purpose of identification.

    e. When identity documents presented by the customer appear altered or when document security features cannot be validated or when the integrity of the document for any other reason is suspected.

    f. When the customer refuses or unable to comply with any aspect of the FI's established non face-to-face onboarding procedures. The customer cannot be onboarded using non face-to-face mode if customer fails to cooperate with full completion of the FI's established non face-to-face onboarding procedure. Such non-compliance can take many different forms including but not limited to a refusal or inability to adjust ambient lighting, a refusal or inability to remove anything that obscures a clear view of the customer's face, customer refusal or inability to remain still or to still the image capturing device, a refusal or inability to answer questions posed by the onboarding officer(s).

    g. When a failure of FI systems prevents the FI from fully executing their established non face-to-face onboarding procedures to include, for example, recording and secure storage of onboarding video and image captures of identity documents.

    h. When the claimed identity cannot be shown to exist using the DRP electronic interface.

    i. When details of the customer's claimed identity are not consistent with details obtained for the claimed identity through the DRP electronic interface.

    j. When a non face-to-face customer presents a NIC with a photo image which the onboarding officer matches with data and imagery from the DRP but which the officer cannot positively match with the current appearance of the customer claiming the identity.

    k. When a non face-to-face customer appears to have intentionally modified his appearance in a manner intended to compromise ability of the FI to accurately identify and verify the customer and to fully complete its established non face-to-face onboarding procedure.

l. When a claimed identity cannot be authenticated to the customer due to an inability to match with a high degree of confidence the images obtained of the customer and of customer identity documents with corresponding images obtained from DRP.

m. When the FI has reason to doubt the veracity of any customer claims, whether related to identity or otherwise.

n. When customer behavior causes the FI to doubt the legal intents or purposes of the customer in establishing business relations.

o. When the FI is unable to identify the current location (eg. using GPS or any other suitable mechanism to identify the location and to determine whether customer is a resident or a non-resident) of the customer by the FI.

p. Where the FI has a reasonable suspicion on the document authenticity in any manner.

10. Policies, Training, Record Keeping and Audit

    a. The FI must establish clear policies and procedures for non face-to-face customer identification and onboarding prior to applying the alternate methods described herein.
    b. The FI must conduct at least an entry level training programme and carry out ongoing training for relevant onboarding staff prior to applying the alternate methods described herein.
    c. FI records that are unique to the alternate methods of customer identification and onboarding contained herein are fully subject to CDD rules regarding record keeping and must be retained in a form sufficient for an internal or external auditor to independently reconstruct the full identification process for any specific customer. Retention of video images is recommended. In the case when a suspicion related to customer identity is formed, the retention of video is mandatory.
    d. FI customer identification programmes using the alternate methods described herein must be included in the FI's internal audit scope under Anti Money Laundering and Combating the Finance of Terrorism (AML/CFT) aspects in order to determine efficacy of the programme and to detect operational deviations from policy.

Part IV - Risk Management

11. The non face-to-face methods of identity verification described herein must be considered in the context of the FI's "risk-based approach" prior to use. If necessary, the FI's risk assessment must be updated to reflect the impact of the non face-to-face methods.

12. Customer risk profiles must reflect any non face-to-face methods of identification used for the purpose of their identification.

13. Customers identified using non face-to-face methods described herein should be monitored and managed as higher risk and subject to enhanced CDD until such time as they are able to present an original identification and the FI is able to verify and make a copy thereof.

14. In addition to the above requirements of treating non face-to-face onboarded customers as of high risk, customers located outside of Sri Lanka must be risk managed in accordance with the known risks of the jurisdiction where the customer is located.

Part V – STR Reporting

15. The entirety of the circumstances, most especially those related specifically to non face-to-face customer identification, must be considered in order to determine whether filing a suspicious transaction report with the FIU is warranted in relation to non face-to-face customer onboarding.

16. Such circumstances may include but not limited to impersonation, any doubt on document authenticity, forged ID and address verification documents, altered ID or address verification documents, altered images, spoofing, reluctance to cooperate or provide additional information for verification, suspicious behavior, discrepancies in information provided.

Part VI - Enforcement

17. The FIU will forbear on enforcement of Schedule to the CDD Rules under Rule 27- Items (1) (b)(i) and Schedule to the CDD Rules under Rule 27- Item (1) (b)(ii) when:
    a. the non face-to-face methods of customer identification contained herein are applied to a particular individual customer, and;
    b. this Guidance is strictly followed in its entirety by the FI; and
    c. this Guidance remains in force.

October 22, 2020