POLICY ON ANTI-MONEY LAUNDERING, COMBATING OF TERRORIST FINANCING AND CUSTOMER DUE DILIGENCE

Version 7.0

Version	Date Approved by the Board Integrated Risk Management Committee	Modification Summary
1.0	05th June 2018	Previous AML Policy of the Bank was replaced with the new version that included the Risk Based Approach on Anti Money Laundering, Suppression of Terrorist Financing and Customer Due Diligence
2.0	04th June 2019	Annual Review – No Changes
2.0	July 2020	Previous Policy on Risk Based Approach for Anti Money Laundering, Suppression of Terrorist Financing and Customer Due Diligence – Version 2.0 was replaced with the following new additions. i. Amended the Predicated Offenses List in line with the Amendment No 40 of 2011 to the Prevention of Money Laundering Act No 05 of 2006 ii. Inclusion of PEP identification categories in line with Guideline No. 03 of 2019 issued by the Financial Intelligence Unit iii. Inclusion of procedure to be followed on Non -face to face customers
3.0	14th October 2021	The Policy has been amended with the following to provide better clarity. i. Inclusions were made covering Standards, Legislation and Regulatory requirement ii. Inclusions on fines and penalties imposing to the bank and to the Employees iii. Inclusion on the Compliance Structure in the three lines of Defense Model iv. Responsibility of all Staff on AML/STF v. Process on Annual Review of the PEP Customers vi. New additions on the High Risk Customers vii. Manual transactions monitoring based on exceptional reports.
4.0	13th October 2022	The Policy has been amended with the following to provide better clarity. i. Inclusions were made covering requirement on the New Financial Crime Management System ii. Inclusions were made covering Standards, Legislation and Regulatory requirement

5.0	17th May 2023	The Policy has been amended with the following. Amending the AML policy, on timing of the screening of the existing customer database from quarterly basis to as and when a designated list is published and existing customer base to be screened once in two weeks. ii. Inclusions were made to the Bank's policy to exclude some categories from entering into financial relationships. Accordingly the Bank will not enter into financial relationships with the individuals with matching NICs to fraudulent NICs published by the Department of Persons Registration (DRP) and individuals and entities engaged in scams as identified and communicated by the director FIU with the Compliance Officer of the Bank. iii. The approving authority to onboard a customer was changed from CEO to COO.
06.	29th July 2024	Annual Review – No Changes
07.	11th Nov 2024	Review – The AML Policy of the Bank reworded and restructured for better clarity. The below Policies were incorporated. Customer on boarding from remote locations The de-classification of PEPs Compliance and Enforcement Multiple Accounts Delayed verification Reliance on Third-Party for CDD Using New Technologies Implementation of AMI/CFT measures on parties involved with online payment platforms Customer Identification and Verification Procedures Ongoing Monitoring of Customer Relationships Transaction Monitoring Sanction Screening Program

Contents

Preamble

Banks and other financial institutions may be used as intermediaries for depositing, safekeeping or transferring of funds derived from criminal activity or financing terrorism. Public confidence in banks' stability can be undermined by adverse publicity as a result of inadvertent association with criminals/terrorists.

Therefore, absence of sound policies, guidelines and practices of managing Money Laundering (ML) and Terrorist Financing (TF) may expose the banks to serious risks.

Recent developments, including robust enforcement actions taken by regulators, corresponding direct and indirect costs incurred by banks due to their lack of diligence have highlighted those risks associated with the failures.

In addition to incurring fines and sanctions by regulators, could result in significant indirect financial costs to banks through the termination of wholesale funding and facilities, claims against the bank, investigation costs, asset seizures and freezes and loan losses.

Therefore, it is of paramount importance that the Bank's Policy of Risk Management on AML/STF is set to be in line with the internationally accepted best practices as well as the domestic legislative and regulatory framework.

DFCC is committed to the highest standards of anti-money laundering compliance within the bank and it's a mandatory requirement for all the employees to adhere to standards and procedures described in the Policy Manual to prevent the use of DFCC's products, services and operations for money laundering and terrorist financing purposes.

In line with above, DFCC has adopted an Anti Money Laundering, Suppression of Terrorist Financing and Customer Due Diligence Policy Manual which provides the basis for all employees to comply with all relevant requirements in this area and assists employees in preserving the good name and reputation of Bank.

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

1. Introduction

1.1. Purpose of the Policy

The policy is termed AML policy herein after for easy reference.

Primary purpose of this Policy is to establish a comprehensive framework for DFCC Bank PLC to effectively identify, prevent, and report Money Laundering (ML), Terrorist Financing (TF) and Financing of Proliferation (FP) activities. This policy outlines the Bank's commitment to comply with all governing AML/CFT (Anti Money Laundering / Countering the Financing of Terrorism) laws and regulations, ensuring that DFCC Bank comply with all governing regulations to manage and mitigate the Compliance risk arising from ML/TF.

Compliance risk is the risk that arises due to non-compliance with applicable laws, regulations, standards, and internal policies. It can manifest in various forms, including regulatory, legal, financial, and reputational risks.

The bank employs a three-line-of-defense mechanism to manage compliance risk effectively. The Compliance Department serves as the second line of defense within this framework.

1.2. Scope of the Policy

This AML Policy applies to all employees, officers, directors, and relevant counterparties of DFCC Bank. It encompasses all products, services, customer interactions, and transactions conducted by the Bank. The Policy ensures a unified approach to AML/CFT compliance across all areas of the Bank's operations.

As stipulated in the Financial Institutions Customer Due Diligence Rules (CDD) No 01 of 2016 the Bank is adopting "Risk Based Approach" (RBA) for the purpose of identifying, assessing and managing money laundering, terrorist financing risks, financing of proliferation.

1.3. Compliance with Laws and Regulations

DFCC Bank is committed to adhering to the AML/CFT and other crimes related laws and regulations of Sri Lanka, including but not limited to the Financial Transaction Reporting Act, the Prevention of Money Laundering Act, Convention on the Combating of Terrorist Financing Act, the Customer Due Diligence (CDD) Rules and any other Rules, Directions, Guidelines as applicable that are issued by the Financial Intelligence Unit of Sri Lanka (FIU Sri Lanka). The Bank also aligns its policies with international standards set by the Financial Action Task Force (FATF) and other relevant global bodies as applicable.

Further details of predicate offences, as outlined in the governing regulations, are provided in Annexure III of this policy.

2. Governance and Oversight

The bank has established a robust and effective corporate governance framework that ensures transparency, accountability and high ethical conduction all aspects of their operations. Further a sound corporate governance framework that includes effective policies and procedures, monitoring and reporting mechanisms and internal controls are in place.

In the Bank's AML/CFT governance structure comprises of the Chief Compliance Officer directly reporting to the Board Integrated Risk Management Committee (BIRMC) chaired by an Independent Director of the Board as stipulated by the Corporate Governance regulations. The BIRMC meetings are held once in two months or as appropriate and BIRMC is responsible for overseeing the Bank's AML/CFT strategies, ensuring continuous improvement. The BIRMC minutes are submitted to the Board of Directors for the required appraisals. The AML Policy is recommended for approval of the Board by the BIRMC and submitted for the approval of the Board of Director's of the Bank.

2.1 Board Responsibilities

The Board of Directors holds ultimate responsibility for the effectiveness of DFCC Bank's AML/CFT program. Senior management is tasked with implementing the Board's directives, ensuring that AML/CFT policies are integrated into the Bank's operations, and fostering a culture of compliance throughout the Bank. Such a responsibility should safeguard the Bank from any regulatory risk stemming from the stated regulations. Accordingly, the Board shall;

i. Establish the institution's overall risk appetite in relation to AML CFT and should ensure that mechanisms are in place to effectively mitigate risk.
ii. Ensure that appropriate policies, procedures and controls are in place to manage such risks and approve the same.
iii. Understand the legal regime and regulatory environment governing the Anti Money Laundering Laws and Combating of Terrorist Financing.
iv. Ensure that Bank takes appropriate steps to identify, assess and manage its Money Laundering and Terrorist Financing Risks.
v. Appoint a Senior Management level officer as the Compliance Officer, who shall be responsible for ensuring Bank's compliance with the requirements of the AML/CFT rules.
vi. Should also ensure that arrangements are in place for the effective reporting on all such issues related to the functioning of the risk management framework and ensure that timely reports of Bank's risk assessment on money laundering and terrorist financing risk profiles, effectiveness, and risk control and mitigation measures are received by the Board.
vii. Ensure that Compliance Officer and staff of the Compliance Department have prompt access to all customer records and other information required to discharge their duties under AML and CFT.
viii. Maintain an independent audit function in order to effectively assess Bank's internal policies, procedures and controls over AML and CFT.
ix. Ensure the Compliance function is equipped with appropriate systems and resources.

2.2 Responsibilities of the Senior Management

Senior management should demonstrate a firm understanding of all aspects of the institution's AML /CFT framework 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 AML/CFT risk. They are also responsible for ensuring that effective communication and reporting arrangements are in place to support good risk management practices.

Further Senior Management shall ensure that intensity and extensiveness of risk management of ML and TF shall be in compliance with "risk based approach" and be proportionate to the nature, scale and complexity of the Bank's activities.

i. Ensure that the Compliance officer or any other person authorized to assist the Compliance officer has prompt access to all customer records and other relevant information which may be required to discharge the duties of the Compliance function.

ii. Ensure developing and implementing of comprehensive employee due diligence and screening procedure.

iii. Support the Compliance Officer to implement suitable training for employees including Board of Directors.

iv. Ensure that Bank identify, assess and take appropriate measures to manage and mitigate ML and FT risks pertaining to following,

   a. New products
   b. Services
   c. New business practices,
   d. New delivery channels
   e. New technology development for new and existing products

2.3 Responsibilities of the Compliance Officer

The Compliance function at the Bank is responsible for ensuring that the Bank effectively identifies, measures, monitors, controls and mitigates ML/TF risks. From a day-to-day operational perspective Compliance function shall ensure that the ML/TF risk management objectives are achieved.

The Compliance function is headed by the Compliance officer and in terms of the Financial Transaction Reporting Act No. 6 of 2006 section 14, Compliance Officer's responsibilities shall primarily be to develop and enforce the Bank's Anti-Money Laundering and Combating of Terrorist Financing Policy, which will include the following;

i. Customer identification requirements
ii. Record keeping and retention requirements

iii. Requirements for conducting ongoing due diligence on business relationships and ongoing scrutiny of transactions throughout the business relationship
iv. Reporting requirements including reporting of suspicious transactions and customer transactions.
v. Ensure requirements of screening new staff before hiring them as employees.
vi. Keep Board, Management & the staff informed of new regulations issued in relation to AML/CFT
vii. Conduct required staff training.
viii. Monitoring of transactions.
ix. Implement process and systems to enforce effective transaction screening process
x. Submission of regulatory returns.
xi. Act as a Regulatory contact point.
xii. Provide timely information to the Board/BIRMC and to the Management on the status of AML/CFT risk of the Bank for their appraisal.

2.4 Responsibility of all Staff

i. All employee of the Bank are responsible to ensure the prevention of money laundering and combating of terrorist financing on a day to day basis and to ensure the implementation and adherence of procedures and controls that meet the requirements of this policy and related policies and guidelines issued by the Compliance Department.

ii. Staff members who become aware of breaches of this policy shall raise/escalate such breaches through the procedure laid down in the Bank's Whistle Blowing Policy.

iii. Most of the provisions in this Policy as well as the other Guidelines issued by the Compliance Department involve detailed and/or technical requirements. Any employee requiring clarification regarding any matter in this Policy Manual or concerning any other money laundering or terrorist financing matter, or wishing to provide feedback or suggestions for updates to the Manual, should contact Compliance Officer of the Bank.

iv. Compliance and Enforcement
Non-compliance with this AML Policy or any instructions issued by the Compliance Department in relation to same shall be considered a violation of the Bank's policies and may result in disciplinary action, up to and including termination of employment as required, in accordance with the Bank's disciplinary procedures.

3. Customer Due Diligence (CDD)

3.1 Policies on Customer Due Diligence

Bank shall develop and implement clear customer acceptance policies and procedures to identify the types of customers that are likely to pose a higher risk of ML and FT pursuant to the bank's risk assessment.

Such policies and procedures should require basic due diligence for all customers and commensurate with the due diligence required for the level of risk associated with the customer. For proven lower risk situations, simplified measures may be permitted to the extent given by CDD rules. Where the risks are higher, the bank should conduct Enhanced Due Diligence (EDD) measures to mitigate and manage such risks.

Bank's basic customer acceptance policy is set forth below. Detailed procedures relating to CDD shall be communicated as required from time to time in respective manuals, guidelines and instructions. Such policies, procedures and controls shall include, risk assessment procedures, CDD measures, manner of record retention.

i. The Bank shall conduct the CDD measures as regulated at the point of on boarding a customer (Customer due diligence) and when conducting transactions with customers (Transaction due diligence) under all circumstances and especially in the following instances.

    a. Entering into business relationships
    b. Providing money and currency changing business for transactions
    c. Providing wire transfer services
    d. Carrying out occasional transactions involving an amount exceeding rupees two hundred thousand 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 the Bank has any doubt about the veracity or adequacy of previously obtained information.

ii. The Bank shall

    a. Identify its customers prior entering into business relationships
    b. Obtain the information specified in the CDD Rules, verify such information, as applicable and record the same for the purpose of identifying and initial risk profiling of customers, obtain the following information for the purpose of conducting CDD, at minimum

        a. Purpose of the account
        b. Sources of earning

c. Expected monthly turnovers
d. Expected mode of transactions (ex; cash, cheque, etc.)
e. Expected type of counterparties (if applicable).

iii. The Bank shall obtain documents as specified in the CDD rules based on the type of the customer on boarded which is mentioned in the Operations manual of the Bank.

a. Bank shall not open, operate or maintain any anonymous account, any account in a false name or in the name of fictitious person or any account that is identified by a number only.
b. Bank shall not operate and maintain accounts where the ownership is transferable without the knowledge of the Bank.
c. Bank shall not operate and maintain accounts where the account holder's name is omitted.
d. Bank shall maintain accounts and information in a way that assets and liabilities of a given customer can be readily retrieved.
e. Bank shall not maintain accounts separately from the Bank's usual operational process, systems and procedures.
f. Bank shall conduct CDD measures as specified in rules issued by FIU from time to time and any other appropriate guidelines that are proportionate to the nature, scale and complexity of Bank's activities and ML and TF risk profile.
g. Bank shall not enter into relationship with certain business categories. Refer Annexure III of the Policy for Excluded and High Risk Customer Categories and EDD measures.
h. Further, Bank shall conduct Enhanced Due Diligence when entering into relationship with High Risk Customer categories. Inability to comply with CDD measures
i. Where the Bank is unable to comply with the relevant CDD measures, the Bank shall,
    i. In relation to a new customer, not open the account or enter into the business relationship or perform the transaction or
    ii. In relation to an existing customer, terminate the business relationship, with such customer and consider making a suspicious transaction report in relation to the customer.

Under no circumstances shall, the Bank 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.

3.1.A Legal Persons, Legal Arrangements, and Beneficial Owners

The Bank shall, in the case of a customer that is a legal person or legal arrangement,

i. Understand the nature of the customer' s business, its ownership and control structure
ii. Identify and verify the customer in terms of the requirements as required in the CDD Rules.
iii. Where one or more natural persons are acting on behalf of a customer

    a. The Bank shall identify the natural persons who act on behalf of the customer,
    b. Understand the ownership structure of the customer and determine the natural persons who ultimately own or control such customer and verify the identity of such persons.
    c. 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.
    d. Where there is a beneficial owner (who owns more than 10%) 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 it knows who the beneficial owner is.
    e. In order to identify the natural person, the Bank shall at the minimum obtain and take reasonable measures to verify the following;

iv. Identity of all Directors and Shareholders with equity interest of more than ten per cent with the requirement imposed on the legal person to inform of any change in such Directors and Shareholders.
v. 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
vi. Authorization given for any person to represent the legal person or legal arrangement either by means of Board Resolution or otherwise
vii. Where no natural person is identified under the preceding provisions, the identity of the relevant natural persons who hold the positions of senior management
viii. When a legal person's controlling interest is vested with another legal person, Financial Institution shall identify the natural person who controls that legal person.

When the customer is a legal arrangement

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

i. 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

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

The Bank complies with the Guidelines for Financial Institutions on Identification of Beneficial Ownership, No. 04 of 2018 at all times.

3.1.B Customer Risk Assessment at the Time of Client On-boarding

In terms of Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 by Gazette Extraordinary No 1951/13, dated January 27, 2016, bank shall take appropriate steps to identify access and manage its money laundering and terrorist financing risk in relation to its customers.

In line with the above guideline, it is a requirement of Account Opening Officers/ Relationship Managers to assess the customer in order to identify Money Laundering and Terrorist Financing (ML/TF) risk at the time of client on boarding.

Account Opening Officers/ Relationship Managers should be mindful that the risk profile of a customer is variable and will depend on several risk factors as detailed below.

i. Customer Type
ii. Occupation/Business
iii. Jurisdiction/ Geographic Area
iv. Products /Services
v. Delivery Channels
vi. Expected Turnovers
vii. Source of funds
viii. Identification of Ultimate Beneficial owners
ix. PEP Status.

In order to comply with the above requirement, ML/TF Risk Assessment on customers should be conducted based on the above parameters at customer level (CIF) which has been developed through KC+ Module of the Financial Crime Mitigation System (FCM).

The Bank does not establish financial relationships with customers whose risk profiles exceed its defined tolerance levels. The specific categories of such excluded customers are outlined in Part I of Annexure IV of this policy.

Additionally, certain customers with a high risk of Money Laundering (ML) or Terrorist Financing (TF) may be on-boarded subject to Enhanced Due Diligence (EDD). Details regarding these customers are provided in Part II of Annexure IV.

3.1.C Customer On-boarding from Remote Locations

Accounts should generally be opened at the branch closest to the customer's residence or primary place of business. Remote account openings are permitted only under specific circumstances, requiring valid justification and appropriate approvals. The Bank's stipulated procedure shall be followed at all times in relation to such remote on boarding.

3.1.D Multiple Accounts

If a customer opens two or more accounts, the specific purpose for which such accounts are opened should be clearly recorded.

3.1.E Occasional Customers, One-off Customers, Walk-in- Customers and Third Party Customers

With regard to Occasional Customers, One-off Customers, Walk-in- Customers and Third Party Customers in the following instances the bank shall conduct CDD in line with the CDD rules.

i. Transactions or series of linked transactions exceeding rupees two hundred thousand or its equivalent in any foreign currency conducted.

ii. When they wish to purchase remittance instruments such as pay orders, drafts exceeding rupees two hundred thousand or its equivalent in any foreign currency,

iii. With regard to **all cash deposits** exceeding rupees two hundred thousand 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.

3.1.F NGO and Non Profit Organizations and Charities

Bank shall apply enhanced due diligence measures to NGO, NPO and Charities. CDD should also be conducted on office bearers and authorized signatories of the entity as follows;

i. The Bank shall open accounts in the name of the relevant NGO, NPO or Charity as per title given in the constituent documents thereof.
ii. The individuals who are authorized to operate the accounts and members of their governing bodies shall also be subject to enhanced CDD measures.
iii. The Bank shall ensure that the persons who are authorized to operate the accounts and members of their governing bodies are not affiliated with any entity or person designated as a proscribed entity or person, whether under the same name or a different name.
iv. No Financial Institution shall 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.

v. The Bank shall at a frequency determined 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 proscribed entity and person, either under the same name or a different name.
vi. The Bank shall conduct enhanced CDD measures when entering into a relationship and conducting transactions with NGO, NPO or Charities to ensure that their accounts are used for legitimate purposes and the transactions are commensurate with the declared objectives and purposes.
vii. In case of any suspicion on similarity in name or possible ML/TF risk the Bank shall file a Suspicious Transaction, Report or take other legal action or both.
viii. Further Circular No. RAD/99/01 issued by the Secretary to the President on 06.02.1999 requires all international and national level **foreign funded** voluntary social services organizations/Non-Governmental Organizations (NGOs) to re-register with the National Secretariat for Non-Governmental Organizations. Thus such registration shall be verified at the point of on boarding such entities or when they do foreign denominated transactions.

Accordingly, the Bank is required to monitor and report any Non-Governmental Organization,

i. Not registered with the National Secretariat for Non-Governmental Organizations, and
ii. Receives direct foreign funds / remittances into their accounts.

The Bank may submit such report under Section 7 of the Financial Transactions Reporting Act, No. 06 of 2006

3.1.G Non - Face to Face Customers

A non-face-to-face transaction is where a transaction occurs without a customer having to be physically present. As such Bank shall apply enhanced due diligence measures and risk profiling on customer considering the products, transactions or delivery channels of the non face to face customer. Further Bank shall have in place proper customer verification mechanism process in line with the given regulation as applicable.

Non face to face customer on boarding shall have proper control to mitigate fraud risk, laundering risk and terrorist financing Risk.

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

3.1.H Customers and Financial Institutions from High Risk Countries

Bank shall apply enhanced due diligence measures to customers from high-risk countries.

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 suppression of terrorist financing policies and not making sufficient progress in addressing those deficiencies in those countries as per the information in the information through public domain.

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 corresponding to the nature of risk of listed high risk countries.

i. Limiting business relationships or financial transactions with identified countries or persons located in the country concerned;
ii. Review and amend or, if necessary, terminate, correspondent banking relationships with Financial Institutions in the country concerned;
iii. Conduct any other measure as may be specified by the Financial Intelligence Unit.

3.1.I Politically Exposed Persons

Bank shall apply enhanced due diligence measures to Politically Exposed Persons and perform regular adverse/negative news checks to identify potential risks related to money laundering or terrorist financing. Bank will **adopt** the Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019 issued by the Financial Intelligence Unit on 01st October 2019 for identification of PEPs. In terms of Section 08, 09 and 10 of the guideline Bank will consider following categories as PEPs

i. Domestic PEPs: individuals who are entrusted with prominent public functions in Sri Lanka.
ii. Foreign PEPs: individuals who are entrusted with prominent public functions by a foreign country.
iii. International organization PEPs: persons who are entrusted with a prominent function by an international organization.
iv. Immediate Family members: individuals who are related to a PEP either directly (on grounds of consanguinity) or through marriage or similar (civil) forms of partnership.
v. Close associates: individuals who are closely connected to PEP, either socially or professionally.
vi. immediate family members of PEPs include any of the following relations:

    a. Spouse (current and past)
    b. Siblings, (including half-siblings) and their spouses
    c. Children (including step-children and adopted children) and their spouses
    d. Parents (including step-parents)
    e. Grand children and their spouses.

vii. Close associates of PEPs or their family members includes;

    a. A natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship with any person identified in FIU guidelines 7 or 9 on PEPs
    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 identified in FIU guidelines 7 and 9 on PEPs

c. A PEP's widely- and publicly-known close business colleagues or personal advisors, in particular, persons acting in a financial fiduciary capacity.

Bank will also adopt the Non-Exhaustive List Categories of Customers that can be considered as PEPs mentioned Annexure A to the above FIU Guideline on PEPs.

Officers are required to obtain prior approval from the Chief Operating Officer (COO) or in the absence of COO from Vice President - Branch Operations for entering in to relationship with PEPs. In order to get the COOs approval the branch should first get the Compliance clearance and then Branch Operation's clearance to be obtained.

In case of entering into relationship the status of PEP is not identified due to whatsoever reason or the customer becomes a PEP subsequently to entering into relationship, respective Branch or Relationship Manager shall obtain post approval from COO and in the absence of COO from Vice President - Branch Operations for continuation of the relationship.

Account officer shall ensure to tag the PEP customer in the T24 at the time of on boarding the PEP customer.

Annual Review of the PEP Customers: In terms of the regulation No. 03 of 2019, PEPs shall be subject to annual review and Enhanced Due Diligence (EDD) shall be carried out by the RM/Branches. Relevant Branches /RMs are required to carry out PEP annual reviews on the standard format shared by Compliance Department.

The de-classification of PEPs

The de-classification of PEPs will be determined on a case-by-case basis, and it has no specific pre-agreed time period. The decision to de-classify a PEP will be made by the Compliance Officer. Any de-classification will require the prior written approval of the Compliance Officer.

The below table provides the indicative classification of time limits on the un-tagging of PEPs after ceasing active public functions.

Category as per the PEP guidelines No. 03 of 2019	Description	Time Limit
A	A head of a State or a Government	No time limit is applicable. PEP status will continue.
B	A politician	No time limit is applicable. PEP status will continue.
Identified categories from C to H	Decided based on a risk based approach.	No time limit is applicable. PEP status will continue.
Other categories included in the PEP guidelines would be treated as below.		
C	A senior government Officer	PEP status will continue for further period of 5 years after permanently ceasing to be in active PEP status. Thereafter a risk based approach has to be followed consisting of the followings. i. When dealing with a former PEP representing ii. These categories, the Bank should focus on the iii. Actual risks. Mainly considering the level of iv. Influence the person still can impose, how v. Influential they were in their previous role, and if vi. Their old and new jobs are connected in any way. vii. Continue to monitor the activities and transactions viii. By delisted PEPs by maintaining high risk status in ix. The core banking system. However delisting customers will be done with the prior written approval of the Compliance Officer.
F	Senior officers into Foreign service	
G	A senior executive of a State owned Corporation	
H	A senior executive of a State owned Government	
I	Foreign PEPs	No time limit is applicable. PEP status will continue.

3.1.J Agency Functions of Money or Value Transfer Service Providers (MVT'S)

i. Bank shall act with enhanced due diligence when entering, sending and receiving funds through money remittance services owing to its inherent risk when paying and receiving funds to/from third parties.
ii. Bank has to ensure that MVTS providers are guided by provisions of the CDD gazette in terms of wire transfers.

iii. Business promotion officers shall at all times obtain the approval/clearance of the Board, Senior Management and Compliance Officer before establishing relationship with any money remittance services.
iv. Business promotion officers should ensure that every precautionary measure is made to distinction between formal money transfer services and other alternative money value transfer systems through which funds or value are moved from one geographic to another, through informal and unsupervised networks or mechanisms.
v. 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.
vi. This Policy shall be applicable to all agents and shall comply with the bank's CDD requirements when accepting cash and when making payments and respective Procedure manuals/guidelines issued by the Bank and/or the respective money remittance service.
vii. Adequate training shall be provided to agents by the business line, on their responsibilities and all aspects regarding identification, checking and approving transactions, recording, reporting and retaining records.

3.1.K. Correspondent Banking Relationships

Staff members who are responsible for establishing and maintaining correspondent Banking relationship shall ensure adequate information is obtained from the respective entity prior to entering into relationships and / or from time to time as informed by the CDD Rules.

Staff members responsible for correspondent bank relationships shall ensure that the Bank does not undertake business with shell financial institutions and ensure that no accounts for shell financial institutions are opened by the Bank. Staff members should ensure to conduct annual reviews on the correspondent banks & RMAs.

The Bank is committed to managing the risks associated with money laundering and terrorist financing, particularly in correspondent banking relationships. As part of this commitment, the following measures must be applied when providing correspondent banking services to respondent banks.

i. Risk Management
The Bank shall take necessary measures to ensure that the risk of money laundering and terrorist financing is adequately managed in correspondent banking relationships, including ensuring that respondent banks do not engage in illicit activities, such as being used by shell banks.

ii. Assessment of Respondent Banks
The Bank shall assess the suitability of any respondent bank by gathering adequate information, including:
    a. Anti-money laundering (AML) and counter-terrorist financing (CTF) policies of the respondent bank.
    b. Information regarding management, ownership, business activities, and geographical presence.
    c. Measures in place to prevent and detect money laundering.

d. The purpose of the account or services provided.
e. Identity of third parties using the correspondent banking services (for payable-through accounts).
f. The regulatory environment in the jurisdiction of the respondent bank.

iii. Due Diligence

The Bank shall

a. Review publicly available sources to assess the reputation and supervision of the respondent bank, including whether it has been subject to any money laundering or terrorist financing investigations.
b. Evaluate the adequacy and effectiveness of the respondent bank's AML and CTF systems based on the regulatory standards of its jurisdiction.
c. Document and clearly understand the respective responsibilities of both the Bank and the respondent bank in relation to AML and CTF.
d. Obtain prior approval from the Board of Directors of the respondent bank before entering into new correspondent banking relationships.

iv. Payable-Through Accounts

The Bank shall ensure that, in cases of payable-through accounts, the respondent bank:

a. Has conducted Customer Due Diligence (CDD) measures on customers who have direct access to the correspondent bank's accounts.
b. Can provide relevant CDD information upon request.

v. Enhanced Due Diligence

The Bank will apply enhanced CDD measures when dealing with correspondent banking relationships involving high-risk jurisdictions, as defined in the applicable regulatory guidelines.

vi. Shell Bank Prohibition

a. The Bank will not enter into or continue any correspondent banking relationship with a shell bank.
b. The Bank will take appropriate measures to ensure that respondent financial institutions do not permit their accounts to be used by shell banks.

The Bank does not offer Correspondent Banking services to regulated Money Service Businesses (MSBs)/Money Value Transfer Services(MVTSs)

The Correspondent Bank Compliance Manual outlines the specific steps and due diligence protocols to be followed in this regard. Compliance to the set procedure shall be ensured.

3.1.L Trade Finance

Trade-based Money Laundering and Terrorist Financing usually involve invoice manipulation and use trade finance routes and commodities to avoid financial transparency, laws and regulations. The use of these Trade facilities such as Letters of Credit and other contingency facilities need to be reviewed from time to time by the Trade and relevant Relationship/Branch staff.

Further Trade Transactions are screened against "World Check" (a database consisting of high risk individuals and institutions worldwide) to ensure that transactions with sanctioned countries, vessels, individuals and entities are effectively captured.

All trade facilities/services shall only be offered to customers who maintain accounts with the Bank and whose KYC is in place and subject to Enhance Due Diligence. CDD reviews as per the policy of the Bank to be conducted on all such customers.

3.1.M Treasury Dealings

With regard to dealings in Forex, money market, bonds, securities, precious metals etc. The Bank staff should ensure that the counter-parties adherence to AML/CFT guidelines to prevent transactions being non-Compliant.

3.1.N Wire Transfer Services/Remittances

Extra vigilance is required by the Bank when facilitating money transmission services and other money or value transfer systems through, which the funds or values are moved from one geographic location to another.

This is required in order to ascertain the sources of such funds and the legitimacy of the transaction/s.

Further, Wire Transactions are screened against "World Check" through FCM to ensure that transactions with sanctioned countries are effectively captured.

All Wire transfer services shall only be offered to customers who maintain accounts with the Bank and whose KYC is in place and subject to Enhance Due Diligence

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 an identity 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 the United Nations Act, No. 45 of 1968.
The Bank shall preserve Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages that accompany inward remittances for a period of six years from the date of transaction.

1. **Ordering Party Financial Institution**

When the Bank is functioning as the Ordering Financial Institution the Bank shall ensure that all cross-border to be always accompanied with the Following.

i. Originator information

   a. Name of the originator
   b. 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

c. Originator's address, national identity card number or any other customer identification number as applicable;

ii. Beneficiary information

a. Name of the beneficiary and
b. The 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.
c. 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 to ascertain where there is 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.

The Bank shall maintain all originator and beneficiary information collected, in accordance with the FTRA.

If the Bank functioning as the Ordering Financial Institution fails to comply with the requirements specified in Rules 70 to 75 of the CDD rules as summarized above (both inclusive) in respect of a wire transfer, 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.

2. 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 Intermediary Financial Institution shall keep a record, for at least six years, of all the information received from the ordering Financial Institution or another Intermediary Financial Institution.

The Bank when involved in wire transfers as an Intermediary Financial Institution 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,

i. when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and
ii. what is the appropriate follow up action;

3. Beneficiary Financial Institution

The Bank when functioning as the Beneficiary Financial Institution 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 when functioning as the Beneficiary Financial Institution shall verify the identity of the beneficiary, and maintain the information in accordance with the FTRA if the identity has not been previously verified.

The Bank when functioning as the Beneficiary Financial Institution shall have risk-based internal policies and procedures for determining,

i. When to execute, reject or suspend a wire transfer with insufficient, originator or beneficiary information; and
ii. What is the appropriate follow up action.

3.1.O CCTV Operations for AML/CFT Purposes

As per the Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021 (and subsequent amendments) the Bank has developed a CCTV Policy and CCTV Procedure Manual to mitigate risk of money laundering and terrorist financing risk of the bank. .

In order to enhance the effective usage of the CCTV system, the Bank 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 as determined by the Bank.

3.1.P Guidelines for Financial Institution on Keeping Accounts Reported in Suspicious Transaction Reports under Surveillance, No 01 of 2022.

In terms of FIU Guideline No 01 of 2022, The bank is required to closely monitor the reported accounts informed by the FIU to be Kept Under Surveillance (KUS), for a period of three months, unless specified otherwise and submit a report to the FIU within three working days from the end of the period of three months or the end of the specified period on whether the reported suspicious transactions are continuing or not. Reporting circumstances are below.

i. Customer Requests to close the reported accounts
ii. Significant deposits / withdrawals to/from the reported account not in line with the

declared profile

iii. Change in the transaction pattern/emergency of new trends.
iv. Change of the ownership/control of the reported account
v. Significant changes in KYC/CDD details

3.1.Q Delayed Verification

i. The Bank is required to 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 as mentioned above.
ii. Provided however; where the risk level of the **customer is low** according to 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 conditions allow its customer and beneficial owner to furnish the relevant documents subsequent to entering into the business relationship and subsequently complete the verification.
iii. In any case where delayed verification is allowed the following conditions shall be satisfied.
    a. Verification shall be completed as soon as it is reasonably practicable but not later than fourteen working days from the date of opening of the account.
    b. The delay shall be essential so as not to interrupt the Bank's normal conduct of business; and
    c. No suspicion of money laundering or terrorist financing risk shall be involved.

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

v. The Bank shall take measures to manage the risk of delayed verification which may include limiting the number, type and amount of transactions that can be performed.

3.1.R Reliance on Third-Party for CDD

The Bank is permitted to rely on a third-party Financial Institution or designated non finance business I (Embassies or similar entities) in order to conduct CDD measures, including the identification of the customer, identification of the beneficial owner and understanding the nature of the business or initiating the business. The ultimate responsibility for CDD measures shall remain with the Bank relying on the third party, which shall-

i. Obtain immediately the necessary information relating to CDD;
ii. Take steps to satisfy itself that copies of identification data and other relevant, documentation relating to CDD requirements will be made available from the third party Financial Institution or designated non finance business, upon request without delay;

iii. Satisfy itself that the third party Financial Institution or designated non-finance business is regulated, supervised or monitored, and has measures to adhere to CDD and record-keeping requirements in compliance with the FTRA.

The Bank when relying on third party shall,

i. Have internal policies and procedures which enable the mitigation of anti-money laundering and terrorist financing risks to the international financial system, including those from countries that have been identified by the Financial Action Task Force as having strategic deficiencies in anti-money laundering and suppression of terrorist financing policies.
ii. Have regard to information available on the level of country risk, when determining the country of a third party.

3.1.S Using New Technologies

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.

The Bank shall -

i. Under take the risk assessments prior to the launch or use of new products, practices and technologies;
ii. 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
iii. Not permit pre-loading of credit cards, as that may amount, inter-alia, to the abuse of credit cards, for money laundering and terrorist financing purposes.

3.1.T Implementation of AMI/CFT Measures on Parties Involved with Online Payment Platforms

The Bank when enabling online payment system has the responsibility to ensure that all parties involved with such online payment platforms comply with Financial Transactions Reporting Act, No.6 of 2006 (FTRA), Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 and other rules, regulations, guidelines issued there under in relation to followings, for parties involved with such online payment platforms.

i. Identification and verification of customers
ii. Conduct ongoing due diligence on customers and scrutiny of transactions
iii. Identification and reporting of Suspicious Transactions
iv. Wire transfer requirements (in particular, originating financial institution shall
v. make originator information available to the beneficiary financial institution)
vi. Targeted financial sanctions screening
vii. Record keeping
viii. Other reporting requirements

3.2 Risk Based Approach to CDD

DFCC Bank adopts a risk-based approach to Customer Due Diligence, tailoring its due diligence processes based on the risk profile of each customer. High-risk customers, such as Politically Exposed Persons (PEPs), those who are from high-risk jurisdictions and customers with high-risk profiles undergo Enhanced Due Diligence (EDD) to mitigate potential ML/TF risks.

3.3 Customer Identification and Verification Procedures

The bank ensures accurate identification and verification of all customers through reliable, independent source documents, data, or information. Procedures include,

i. Collecting and verifying identification documents (e.g. valid national identity cards, valid passports, valid driving license or any other acceptable documents to the regulator).
ii. Verifying the authenticity of documents through independent sources.
iii. Maintaining records of customer identification information.

The customer on boarding staff shall be equipped with the necessary knowledge to identify forged or inaccurate identification documents. Additionally, the Bank collaborates with the Department of Registration of Persons (DRP) to verify the authenticity of national identity cards submitted by customers, when required.

3.4 Ongoing Monitoring of Customer Relationships

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 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 of the Bank.

The Bank may 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 its existing customers having, regard to 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, every Financial Institution may consider the following.

i. The nature and circumstances surrounding the transaction including the significance of the transaction
ii. Any material change in the way the account or business relationship is operated or
iii. The insufficiency of information held on the customer or change in customer's information.

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 subject to enhanced CDD measures.

4. AML/CFT Risk Assessment

The on boarding risk assessment of the customers will be conducted in the Financial Crime Mitigation (FCM) system based on the elements such as channel of the customer, Currency, counterparty, Country , PEP/NGO/STR/Freezing order status of the customer, products , source of funds , years of on boarding , anticipated deposit volume.

The ongoing risk of the customers will be maintained in the KIYA AML system based on the elements such as

i. Business Intelligence
ii. Transaction type risk
iii. Transaction trend risk and
iv. Scenario violation risk.

This risk will be updated on a daily basis based on the behavior of the customer's profile scoping to the above mentioned criteria

4.1 Customer Risk Profiling

The Bank evaluates ML/TF risk profiles relating to each customer and based on the results of the risk assessments they are categories into 3 levels. The Risk level of the customer is decided by the Bank using a comprehensive pre-approved format developed for risk profiling of customers.

i. Low ML/TF risk profile customers
ii. Medium ML/TF risk profile customers and
iii. High ML/TF risk profile customers.

4.2 Review of customer risk rating

In terms of FTRA and CDD rules Bank shall carry out continuous customer due diligence to ensure that the transactions carried by the customer thorough his account are consistent with the economic profile known to the bank. In this regard, Bank shall adopt a risk based approach depending on the risk category of the customer and procedural guidelines issued by the Compliance Department. In principle, CDD review of a customer shall be conducted based on the below given periodicity.

Customer Risk Category	CDD frequency
High Risk	Annually
Medium Risk	Every three years
Low Risk	Every Five years

Based on Risk Category allocated to each customer, risk assessment shall be periodically reviewed by the respective branch as per the mentioned period.

4.3 Bank wide AML/CFT Risk Assessment

Bank wide risk assessment based pre-approved format, will be carried out by Compliance Department. Appropriate risk assessment methods, risk matrices, processes and systems shall be developed by Compliance Department towards this purpose and shall be reviewed periodically to ensure adequacy. Results of the risk assessment shall be documented and presented to the BIRMC, annually.

5.0 Transaction Monitoring

Transaction monitoring is critical component of the Bank's AML/CFT framework The Bank shall monitor all business relationships with a customer on an ongoing basis to ensure that the transactions are consistent with the customer's economic profile and risk profile, and where appropriate, the sources of earning.

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.

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 report.

The Bank has deployed a post transaction monitoring system for the above purposes. The Bank is committed to ensuring that all transactions are monitored to detect and mitigate potential money laundering, terrorist financing bribery, and corruption risks. The Bank’s transaction monitoring process is designed to comply with the Financial Transactions Reporting Act, No. 6 of 2006, and other applicable regulations.

Any staff members who come across such transaction inconsistent with these rules shall report the same to the Compliance Officer for appropriate action.

5.1 Transaction Monitoring System (TMS)

The Bank utilizes an automated Transaction Monitoring System (TMS), configured to capture suspicious transactions, particularly those indicative of money laundering and terrorist financing (ML/TF) activities. The TMS is configured to detect suspicious activities using alert mechanisms. The AML system generates alerts which require further scrutiny. The Bank's TMS continuously reviews transactions across all customer operating accounts, including Current and Savings Accounts, Fixed Deposits, Government Securities, Trade Finance, FCBU accounts, Credit Cards, Safety Lockers, Pawning, loans and other financial products.

The TMS integrates customer information obtained during the Know Your Customer (KYC) and Customer Due Diligence (CDD) process to ensure transaction profiles align with each customer's disclosed economic activities.

5.2 Data Quality and Accuracy

The Bank ensures that the TMS has access to accurate, complete, and timely transaction data. Reviews are conducted to verify the data quality and identify any discrepancies that may affect the accuracy of alerts generated by the system.

5.3 Red Flags and Suspicious Activity Detection

The Bank's TMS identifies suspicious transactions based on predefined red flag indicators such as

- Unusual transaction volumes or frequencies.
- Transactions involving high-risk jurisdictions or counterparties.
- Structured transactions designed to evade reporting thresholds.

The Bank ensures that its red flag criteria are regularly updated to reflect the latest regulatory guidelines and emerging money laundering typologies. The system parameters are tailored to the Bank's risk profile, and suspicious activity alerts are calibrated in accordance with the Bank's risk appetite.

Suspicious Transaction Reporting Procedure

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

i. Has reasonable grounds to suspect that any transaction or attempted transaction may
ii. be related to the commission of any unlawful activity or any other criminal offence;
iii. or
iv. Has information that it suspects may be relevant
v. To an act preparatory to an offence under the provisions of the Convention on
vi. the Suppression of Financing of Terrorism Act, No. 25 of 2005
vii. 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 Bank 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.

Accordingly

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

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

iii. Where the staff forms a suspicion of money laundering and terrorist financing risk relating to a customer and it reasonably believes that conducting the process of CDD measures would tip off the customer, he/she shall terminate conducting the CDD measures and proceed with the transaction and immediately file a Suspicious Transaction Report.

iv. Any staff member who becomes aware of a suspicious transaction or an attempt at such a transaction must immediately report it to the Compliance Officer.

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

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

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

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

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

Personal Criminal Liability.

i. As per the anti-money laundering legislation in Sri Lanka, any offence under the Act will give rise to a potential personal criminal liability. Therefore, strong disciplinary

action will be taken against any member of staff who fails, without reasonable excuse, to make a report on a suspicious transaction.

ii. Disciplinary action will also be initiated against any member of staff who blocks, or attempts to block, a report by another member of staff.

Protection of Persons Reporting Suspicious Transactions

No Civil, Criminal or disciplinary or reprisal action shall be initiated against any staff member who reports suspicious activity in good faith in terms of the FTRA and in terms of this Policy and the confidentiality of such reporting person shall be protected

Refer annexure V for examples of suspicious transactions

5.4 Alert Generation and Escalation

The system generated alerts are evaluated by the Compliance department. The Compliance department ensures that alerts are addressed in a timely and efficient manner. The TMS is equipped with an established escalation procedure (work-flow) and required information is gathered from the customer account maintain branch to better understand the customer transactions.

The alerts pertaining to the post transaction monitoring rules will be generated in the KIYA AML system. The alerts will be investigated by the AML Team members and if required the same will be escalated to the branches to obtain further information to furnish the detailed investigations. Upon receiving the responses from the branches, the Compliance user will analyze the same and regulatory actions will be taken, as necessary.

6.0 Sanction Screening Program

The Bank shall verify whether any prospective customer or beneficiary appears on any list of designated persons or entities issued under any regulation made in terms of the United Nations Act, No. 45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism and 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.”.

Sanctioned Policy.

The Bank does not carryout business with sanctioned individuals and entities. The Bank employs a robust sanction screening program to mitigate risks associated with conducting business with sanctioned individuals and entities. The Bank strictly adheres to all

applicable sanctions regulations and maintains a zero-tolerance policy towards conducting business with sanctioned individuals and entities. The Bank's procedures ensure that all high risk transactions are screened against relevant sanction lists before processing.

Implementation Mechanism

The Bank follows a two-stage approach to comply with the sanction screening;

i. First stage is the screening of new customers (at the time of customer on-boarding) against the consolidated list of designated persons and associates, to make sure no such persons are becoming customers of the Institutions.

ii. Second stage is the screening of the entire customer database as and when update notifications are issued by the FIU.

6.1 Scope of Screening

The Bank screens against a wide range of sanctions, including:

i. **Domestic Sanctions:** Sanctions imposed by local regulatory authorities.
ii. **International Sanctions:** Sanctions imposed by international bodies such as the United Nations Security Council (UNSC), the European Union (EU), and the Office of Foreign Assets Control (OFAC).
iii. **Other Relevant Sanctions:** Sanctions imposed by other jurisdictions that may impact the Bank's operations, such as correspondent banking relationships.

6.2 Screening Trigger Points

1. Screening of New Customers at the time of On-boarding

Whenever there is a new account opening for a new customer, the details of that customer are required to be screened against the designated list, and the bank is required to ensure that the customer is not a designated person or entity, before entering into a relationship with the customer.

The Bank is required to identify the beneficiaries and/or beneficial owners of their Accounts / transactions and ensure that no designated persons and associates are beneficiaries and/or beneficial owners of the funds, accounts or other assets.

2. Screening of the Customer Database upon Update Notification by the FIU

As soon as the FIU receives a notice from the UN regarding updates to the UNSCR 2231 list, the FIU will circulate a notification email among the Banks. Whenever there is such notification by the FIU, the Bank is required to perform a full screening of customer base of the Bank against the list.

Other Measures

For transactions involving non-account holders / walk-in customers and third-party customers (such as cheque encashment, pay orders and currency exchanges), the Bank should perform screening before conducting the transaction. For that, adequate mechanisms should be set up to obtain information from such individuals. If the Bank identifies a possible match due to such screening, then the relevant branch should inform the Compliance department immediately for necessary action.

The sanction program utilizes two primary systems.

1. **Financial Crime Mitigation (FCM) System for Real-time Screening**

   The FCM system conducts real-time screening of high-risk transactions, ensuring efficient allocation of resources, including,

   i. New customer on-boarding and existing customer amendments
   ii. Inward and outward remittances
   iii. Inward and outward RTGS transactions
   iv. Trade finance transactions (imports, exports, letters of credit, guarantees, etc.)
   v. Local and foreign drafts

2. **KIYA System for CIF Scanning**

   The KIYA system facilitates Customer Information Files (CIFs) screening.

   CIF screenings are conducted against new sanctions within 48 hours of publishing such lists.

   CIF screening relating to incremented customer base is conducted on a daily basis. Reverse screening is conducted once on a daily basis too.

3. **Manual Screening**

In addition to the Bank's automated real-time screening processes conducted through the FCM system, the Trade and Remittance Departments conduct manual screenings. This manual screening process involves verifying critical information such as beneficiary details, order specifics, port of loading, vessels, and countries of origin/destination. This additional layer of scrutiny is implemented prior to transaction initiation in the T24 system, enhancing the Bank's overall AML/CFT compliance efforts. The Bank uses the FCM system for this purpose.

The Compliance Department performs screenings using the World-Check database relating to the cases which have been submitted for Compliance clearance that require enhanced due diligence.

The screening is conducted on below as well.

i. Remittance Payments (Ex;Western Union, Lanka Money Transfer System (LMT))

ii. Correspondent Banks
iii. Products such as Exchange House Remittances, Lanka Money Transfer System
iv. Service Providers, Agents, Outsourced Service Providers
v. Major Shareholders
vi. Related Parties, Key Management Personnel all other employee categories.

At present both the FCM and KIYA systems are integrated with the World-Check database, a comprehensive source of information on high-risk individuals and entities. This integration enhances the effectiveness of the Bank's sanction screening processes.

7.0 Employee Training and Awareness

7.1 AML/CFT Training Programs

The Bank provides regular training and awareness programs for its employees. This includes training on identifying red flags, understanding transaction monitoring alerts, and escalating suspicious transactions. The Bank's training initiatives aim to enhance the understanding of ML/TF risks among staff and ensure compliance with the Bank's AML/CFT framework.

i. Compliance officer shall be responsible for AML/CFT training to all staff of the Bank Including the Board, Senior Management and shall design appropriate modules. Compliance officer shall conduct training to all staff of the Bank, with the assistance of bank's Training Department. Training will be designed on a Risk Based Approach and training department shall be informed of such categories.
ii. It is the duty of the training department to maintain and retain records of training sessions including attendance records and relevant training materials.
iii. Compliance Officer shall from time to time to disseminate AML related laws or changes to existing AML related policies, shall coordinate with the Operations Department and communicate procedures in respect of AML compliance.
iv. Staff should follow mandated training programs on AML/CFT.

8.0 Record Keeping and Reporting

DFCC Bank policy on record keeping is as follows.

i. 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 six years from completion of such transactions.

ii. 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.

iii. 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 six years commencing from the date on which the business relationship was fulfilled or the occasional transaction was effected.

iv. The records shall be maintained up-to-date and be kept in original or copies with the Bank's attestation

v. The Bank shall retain the above records for a longer period where transactions customers or accounts are involved in litigation or required to be produced in a court of law or before any other appropriate authority.

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

9.0 Policy Renewal

This policy shall be reviewed on annually or as and when required based on the changes in the regulatory changes

Glossary and Definitions

Glossary

AML Anti Money Laundering

STF Suppression of Terrorist Financing

FATF Financial Action Task Force

PMLA Prevention of Anti Money Laundering Act No 05 of 2006

FTRA Financial Transactions Reporting Act No 06 of 2006

FIU Financial Intelligence Unit

RBA Risk Based Approach

CDD Customer Due Diligence

EDD Enhanced Due Diligence

PEP Politically Exposed Person

NGO Non Governmental Organization

NPO Non Profit Organization

UBO Ultimate Beneficial Owner

MTVS Money or Value Transfer Service Providers

STR Suspicious Transaction Report

FCM Financial Crime Mitigation System

RMA Relationship Management Application

Definitions

Compliance risk

Compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities (together, compliance laws, rules and standards)

Money Laundering

Money laundering is the process by which criminals disguise the origins of illegally obtained money, typically by passing it through complex transfers or transactions, making it appear as though it comes from legitimate sources. This process generally involves three stages: placement (introducing illegal funds into the financial system), layering (concealing the source through complex financial transactions), and integration (making the funds appear legally earned by re-entering them into the economy).

Terrorist Financing

Terrorist financing is the act of providing funds or financial support, whether directly or indirectly, to individuals or groups involved in terrorist activities. This financing can come from both legitimate and illegitimate sources and is used to support or carry out terrorist acts, sustain terrorist organizations, or promote extremist ideologies.

Proliferation Financing

Proliferation financing is the act of providing funds or financial services that contribute to the development, manufacture, or acquisition of weapons of mass destruction (WMDs) and their delivery systems, in violation of international laws. This type of financing involves the transfer of funds or resources that enable state or non-state actors to pursue nuclear, chemical, or biological weapons programs.

Politically Exposed Person (PEP)

Individuals who hold prominent public positions, along with their family members and close associates, and who may present a higher risk for potential involvement in corruption or money laundering due to their position and influence.

Customer Due Diligence (CDD)

Procedures conducted to identify and verify the identity of a customer, understand the purpose and nature of the business relationship, and assess the risk level of the customer.

Enhanced Due Diligence (EDD)

Additional scrutiny applied to higher-risk customers or transactions, including PEPs, NGOs, and customers from high-risk jurisdictions, involving more thorough verification and monitoring procedures.

Beneficial Owner

The natural person(s) who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted, with a significant interest in or control over the entity.

Source of Funds

The origin of the funds involved in a transaction or account, which should be identifiable and legitimate, especially for high-value or high-risk accounts.

Suspicious Transaction Report (STR)

A report filed to the Financial Intelligence Unit (FIU) when a transaction appears unusual, inconsistent with a customer's profile, or linked to potential money laundering or terrorist financing.

High-Risk Jurisdictions

Countries or regions identified as having strategic AML/CFT deficiencies by the FATF or other regulatory bodies, which require enhanced scrutiny for any transactions or customers associated with them.

Annexure I

Key Regulations Applicable for the Bank

a. International Best Practices

- **Recommendations of the Financial Action Task Force(FATF)**

The Financial Action Task Force (FATF) which is an inter-governmental body which develops international standards to combat money laundering and terrorist financing issued forty (40) recommendations in 2012 setting the international standards that constitute the basic framework for preventing, detecting and suppressing both money laundering and the financing of terrorism and proliferation.

b. Legislation in Sri Lanka on Anti Money Laundering (AML) and Combating of Financing of Terrorist (CFT)

i. Following Acts form judicious framework on Anti Money Laundering and Suppression of Terrorist Financing in Sri Lanka. These are published in the Bank's Compliance Intranet and also could be accessed through the web site of the Financial Intelligence Unit (FIU).

- **Prevention of Money Laundering Act No 05 of 2006" and amendment Act, bearing No. 40 of 2011 (PMLA)**
- **Convention on the Suppression of Terrorist Financing Act No 25 of 2005 and amendment Acts bearing No.41 of 2011 and No.3 of 2013 (CSTF)**
- **Financial Transactions Reporting Act No 06 of 2006 (FTRA)**
- **All Gazettes, Directions, Circulars, instructions issued by the FIU from time to time**

ii. Significant Obligations arising on the Bank

a. Prevention of Money Laundering Act (PMLA)

i. Section 03 of the 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". "*

Penalty for non-compliance would be a fine not more than three times the value of the property or rigorous imprisonment for a period not less than five years and not more than twenty years.

ii. Section 05 of the PMLA

If any person do not disclose to the FIU, knowledge or information obtained by a person in the course of any trade, business, profession or employment on any Money Laundering Activity also an offence under the Act.

Penalty for non compliances would be a fine not exceeding Rs. 50,000 or to imprisonment of either description for a period not exceeding six months or to both such fine and imprisonment.

iii. Unlawful Activities (Predicated offences under the Prevention of Money Laundering Act Refer Annexure I of this Policy)

If any Bank Employee has knowledge or reasons to believe that funds in any account or any transaction is connected with any of the activities given in the list, such knowledge shall be disclosed to the Compliance Officer immediately

iv. Freezing Orders

Section7 A Police Officer not below the rank of Superintendent of Police or an Assistant Superintendent (in the absence of SP) of Police may issue an Freezing Order prohibiting any transaction (any account/ property /investment) which may have been used or which may be intended to be used in connection with offence

Freezing Order shall be in force for a period of 7 days and will be extended through a court order.

As per the Section 7 (3)of the Act , if any person who acts in contravention of a Freezing Order issued, shall be guilty of an offence subject to the following fines and penalties .

- Fine not exceeding Rs. 100,000 or one and a half times the value of the money in such account, property or investment, or
- To imprisonment of either description for a period not exceeding one year or to both such fine and imprisonment.

Bank staff shall not at any given time allow withdrawing any money or facilitating any transaction in line with above section.

Any attempts to violate such freezing orders by the customer or any other staff member should be informed to the CO immediately

b. Convention on the Suppression of Terrorist Financing Act

The Convention on the Suppression of Terrorist Financing Act (CSTFA) . No.25 of 2005 was enacted to give effect to Sri Lanka's obligations under ***"International Convention for the Suppression of Terrorist Financing adopted by the United Nations General Assembly, dated 10/01/2000"*** **and was further amended under Act No. 41 of 2011.**

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

The Act prohibits the financing of terrorist acts, terrorists and terrorist organizations. Further the CSTFA has provisions for freezing of terrorist financing related assets and forfeiture of such assets.

In many respects terrorist financing is the mirror image of money laundering. In one there is an effort to take bad money and make it good and in the other there is an effort to use good money for bad purposes.

Employees should therefore remain alert to all possible money laundering or terrorist financing situations so as to prevent the products, services and operations of DFCC being exploited. Further if any suspicious transactions are noted, same to be reported to the Compliance Officer as per the procedures detailed in this policy Manual.

c. Financial Transaction Reporting Act (FTRA) No.6 Of 200

Section 5- -Bank shall conduct ongoing due diligence on the business relationship with its customer.

Further ongoing scrutiny of any transaction undertaken throughout the course of the business relationship with a customer to ensure that any transaction that is being conducted is consistent with the Banks' knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds

Section9 – Further under the FTRA, no person should divulge that an investigation into an offence of money laundering is being or is to be conducted.

Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is acceptable as it forms an integral part of the KYC program. Such enquiries should not give rise to tipping off.

Section15(2)- As per the powers vested under Section 15 (2) of the FTRA, the Financial Intelligence Unit (FIU) may direct the Banks not to proceed with any transactions or attempted transaction excluding credit transactions in respect of accounts (including safe

boxes/safe deposit lockers), transactions, CDS accounts or any other business relationships including remittances, maintained by certain individuals/entities.

Section 19- Failure to conform to the requirements in the Act, the Bank shall be liable to a penalty as may be prescribed taking into consideration the nature and gravity of relevant non-compliance: Provided however such penalty shall not exceed a sum of Rs.1 Mn in any given case.

Further, failure to comply with the requirement in the Act will lead to Suspension of the Institution from carrying out business or the cancellation of license and will negatively impact on Bank reputation.

Financial Intelligence Unit (FIU)

a) Under the Financial Transactions Reporting Act No. 06 of 2006, FIU has been established as the regulatory agency to receive, analyze data and empowered by the Act to facilitatethe prevention, detection, investigate and prosecute over the offences of money laundering and financing terrorism.

b) Require institutions to undertake due diligence measures to combat money laundering and terrorist financing.

c) Carry out examinations of all institutions for the purpose of ensuring compliance with rules and regulations

d) Empowered to impose penalties to enforce compliance or on failure to comply requirements of the Act, that includes any regulatory measures including but not being limited to suspension or cancellation of license.

e) FIU has powers to issue Rules , Guidelines , Circulars ect.

As part of its anti-money laundering and suppression of terrorist financing program of the bank, Refer Annexure II for the applicable rules as of date:

Annexure II

Rules, Guidelines, Circulars issued by the FIU

i. Extraordinary Gazette No 1437/24, March 23 of 2006 - Establishment of the Financial Intelligence Unit (FIU)
ii. Extraordinary Gazette No 1555/9, June 25 of 2008 – the requirement under Section 6 (b) to report to the Financial Intelligence Unit every cash and electronic fund transfer made at the request of a customer, where the amount of such transfer exceeds Rupees One Million (Rs. 1,000,000) or its equivalent in any foreign currency.
iii. Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 by Gazette Extraordinary No 1951/13, dated January 27, 2016
iv. Guidelines for Financial Institutions on Suspicious Transactions Reporting, No 06 of 2018
v. Guidelines for Financial Institutions on Identification of Beneficial Ownership, No.04of2018
vi. Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019 issued by the Financial Intelligence Unit on 01st October 2019 for identification of PEPs.
vii. Guidelines for Non Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No.03of 2020
viii. Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021
ix. Guidelines for Financial Institution on Keeping Accounts reported in Suspicious Transaction Reports. Under Surveillance, No 01 of 2022
x. Circular 01/2023 Calling for Due Vigilance on Compliance Lapses
xi. Circular 03/2023 - Reminder on Adherence to previously issued Guidelines and Reporting formats on mandatory reporting under the FTRA
xii. Circular 02/2024 Compliance with the Rules on Customer Due Diligence for Financial Institutions.
xiii. Circular 01/2024 Compliance with the Reporting Requirement under the FTRA Act, No.6 of 2006

Annexure III

Predicated offences under the Prevention of Money Laundering Act

a) Offences under Poisons, Opium and Dangerous Drugs Ordinance (Chapter 218
b) Offences under any law or regulation for the time being in force relating to the prevention and suppression of terrorism
c) Offences under Bribery Act (Chapter 26)
d) Offences under Firearms Ordinance (Chapter 182), the Explosives Ordinance (Chapter 183) or the Offensive Weapons Act No 18 of 1966.
e) Offences under section 83c of the Banking Act, No.30 of 1988;
f) Offences under any law for the time being in force relating to transnational Organized crime;
g) Offences under any law for the time being in force relating to cyber crime;
h) Offences under any law for the time being in force relating to offence against children
i) Any written law for the time being in force relating to offences connected with the trafficking or smuggling of persons;"
j) The Customs Ordinance (Chapter 235) and any Regulation, Rule or Order made there under;
k) The Excise Ordinance (Chapter 52) and any Regulation, Rule or Order made there under
l) The Payment Devices Frauds Act, No. 30 of 2006 and any Regulation, Rule or Order made there under;
m) The National Environmental Act, No. 47 of 1980 and any Regulation, Rule or Order made there under;
n) An offence under any other written law for the time being in force which is punishable by death or with imprisonment for a term five years or more:
o) An act committed within any jurisdiction outside Sri Lanka, which would either constitute an offence in that jurisdiction or which would if committed in Sri Lanka amount to an unlawful activity within the meaning of this Act

Annexure IV

Part I
Excluded Customer categories

Bank shall not open and operate accounts for following categories of business.

a) Persons without proper identification documents
b) Shell companies
c) Front organizations/individuals
d) Individuals/entities whose names appear on sanctioned lists
e) The individuals with matching NICs to fraudulent NICs published by the Department of Persons Registration (DRP).
f) Individuals and entities identified as engaged in SCAMs as identified and communicated by the director FIU with the Compliance Officer of the Bank.
g) Arms, defence, military businesses
h) Gambling customers
i) Marijuana- related Entities
j) Nuclear power
k) Red light businesses/Adult entertainment
l) Unregulated charities
m) Virtual Asset Service Providers

Part II
High Risk Customer Categories

Following types of customer categories shall principally be treated as High Risk and respective Branch Managers/Relationship Mangers who are directly responsible to maintain the relationship with the particular customer shall conduct enhanced due diligence since they pose a potential high risk to the Bank in respect of AML and STF

a) Persons engaged in gaming business such as Casinos/Night clubs
b) Persons engaged in Money exchange business
c) Persons engaged in cash incentive business such as wholesale trading/petrol sheds/ pharmacies/ clothing/ vehicle sales
d) Persons engaged in Gem and Jewels trading
e) Persons engaged in Real Estate business
f) Non Governmental Organizations /Non Profit Organizations/ Charities/Clubs and Associations/ Trusts / Foundations
g) Non face to face customers
h) Politically exposed persons
i) High Net worth individuals1
j) Existing customers if the accounts are active , yet the proper documentation of CDD is not with the bank
k) Customers where profile is not matching with transactions and CDD reviews has not been conducted
l) Customers in High Risk Jurisdictions
m) Correspondent Banking Relationships
n) Treasury Dealings customers

o) Trade Finance Business
p) Persons engaged in Wire Transfers
q) Beneficiaries of a life insurance and other investment related insurance policies
r) Embassies/Consulates
s) Extractive industries

It should be noted that above is not an exhaustive list and Branches shall contact the Compliance Officer in case of doubt as to whether any category is posing high risk.

Enhanced Due Diligence for high risk customers shall include one or more of following methods

a) Gather sufficient information from public domain and/or through customer interviews
b) Establish source of funds and wealth with documentary evidence such as audited or management accounts of business , CRIB reports
c) Obtaining of documentary evidence in case of NGOs in respect of their projects and approval
d) Obtain documentary proof of registration /licensing/certificates in respect of business such as casinos/gem traders etc
e) Customer visits
f) Continuously monitor customer transactions

Branches shall monitor customer transactions / activities / behavior continuously and shall conduct post enhanced due diligence in case if any customer is identified to be High Risk subsequent to opening of account /s.

Annexure V

Examples for suspicious transactions

a) A customer-relationship with the bank that does not appear to make economic sense, for example, a customer having a large number of accounts with the same bank, frequent transfers between different accounts or exaggeratedly high liquidity

b) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal

c) Transactions that cannot be reconciled with the usual activities of the customer for example, the use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business

d) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity

e) Large cash withdrawals from a previously dormant/inactive account or from an account which has just received an unexpected large credit from abroad

f) Frequent address changes by customers/clients

g) Client does not want correspondence sent to home address.

h) Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after he/she has opened an account.

i) Unusual nervousness of the person conducting the transaction

j) Client insists on a transaction being done quickly.

k) Client appears to have recently established a series of new relationships with different financial entities.

l) Client attempts to develop close rapport with staff.

m) Client attempts to convince employee not to complete any documentation required for the transaction.

n) Large contracts or transactions with apparently unrelated third parties, particularly from abroad

o) Extensive and unnecessary foreign travel