POLICY ON RISK BASED APPROACH FOR
ANTI MONEY LAUNDERING,
SUPPRESSION OF TERRORIST FINANCING
AND CUSTOMER DUE DILIGENCE

Version 2.0
### Version Modification Summary

<table>
<thead>
<tr>
<th>Version</th>
<th>Date Approved by the Board Integrated Risk Management Committee</th>
<th>Modification Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>05th June 2018</td>
<td>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</td>
</tr>
<tr>
<td>2.0</td>
<td>04th June 2019</td>
<td>Annual Review</td>
</tr>
</tbody>
</table>
# Policy on Risk Based Approach for Anti Money Laundering, Suppression of Terrorist Financing and Customer Due Diligence

## Glossary

## Preamble

## 1.0 Prevention of criminal use of the banking system for the purpose of money laundering and terrorist financing

### 1.1 What is Money Laundering?

### 1.2 What is Terrorist Financing?

### 1.3 Legislation in Sri Lanka on Anti Money Laundering (AML) and Suppression of Terrorist Financing (STF)

## 2.0 AML and STF Program of the Bank

### 2.1 Applicability of Laws and Customer due Diligence Rules

### 2.2 Risk Based Approach on Customer Due Diligence

#### 2.2.2 Bank wide AML/SFT risk assessment

### 2.3 Responsibilities of the Board on AML/STF

### 2.4 Responsibilities of the Senior Management

### 2.5 Responsibilities of the Compliance Officer

## 3.0 Policies on Customer Due Diligence

## 4.0 Training and Awareness

### 4.1 Responsibility on staff Training and Awareness

## 5.0 Risk Mitigating on Customer Transactions

### 5.1 Transaction Monitoring

### 5.2 Sanction Program

## 6.0 Reporting requirements for Suspicious Transactions

### 6.1 Suspicious transaction reporting procedure:

### 6.2 Confidentiality and Non-disclosure

### 6.3 Personal criminal liability

### 6.4 Protection of persons reporting suspicious transactions

## 7.0 Record Retention
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti Money Laundering</td>
</tr>
<tr>
<td>STF</td>
<td>Suppression of Terrorist Financing</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>PMLA</td>
<td>Prevention of Anti Money Laundering Act No 05 of 2006</td>
</tr>
<tr>
<td>FTRA</td>
<td>Financial Transactions Reporting Act No 06 of 2006</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>RBA</td>
<td>Risk Based Approach</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Due Diligence</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>NGO</td>
<td>Non Governmental Organization</td>
</tr>
<tr>
<td>NPO</td>
<td>Non Profit Organization</td>
</tr>
<tr>
<td>UBO</td>
<td>Ultimate Beneficial Owner</td>
</tr>
<tr>
<td>MTVS</td>
<td>Money or Value Transfer Service Providers</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
</tbody>
</table>
**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 and Terrorist Financing 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, it 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.

### 1.0 Prevention of criminal use of the banking system for the purpose of money laundering and terrorist financing

#### 1.1 Money Laundering

There are many definitions of “money laundering”. A relatively simple and non-technical definition is that it is the conversion of tainted or “dirty money” into respectable assets so as to disguise or conceal the origin of such money and to give it the appearance of having been obtained from a legitimate source. What is meant by “dirty money” is that the cash or other property derived from a criminal activity such as drug smuggling, corruption. The scope of criminal activities for money laundering is ever expanding. The purpose of conversion is to give the appearance that the cash or such other property has been obtained from a legitimate source. As in the case of soiled or dirty clothes being laundering, there is a similar process involved in money laundering.
The process of laundering money basically goes through three stages:

- **Placement** - initial entry of illegally derived funds, usually in the form of cash, (may include the other sources of transactions as well) into the financial system;
- **Layering** – multiple transactions such as transferring funds from one account to several other accounts to conceal the origin and the movement of funds;
- **Integration** – making investments in assets such as real estate or expensive cars etc.

1.2 **Terrorist Financing**

The global attention became more sharply focused on terrorism and the need to arrest its funding after the terrorist attack on the World Trade Centre on 11 September 2001 which is commonly known as 9/11 attack. Extensive action has been taken globally to freeze assets held by terrorist organizations and institute other measures required for combating financing of terrorism.

Given below is the definition for “Terrorist Financing” used by Sri Lanka as recommended by Financial Action Task Force and used by the United Nations International Convention for Suppression of Terrorist Financing.

“Any person commits an offence within the meaning of the convention if that person by any means directly or indirectly, unlawfully or willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

1) An act which constitutes an offence within the scope of and as defined in one of the treaties of United Nations Organization
2) *Any other act intend to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a Government or an international organization to do or to abstain from doing any act”*

1.3 Legislation in Sri Lanka on Anti Money Laundering (AML) and Suppression of Terrorist Financing (STF) is through

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 website of the Financial Intelligence Unit (FIU).

- **Prevention of Money Laundering Act No 05 of 2006” and amendments thereto**
- **Convention on the Suppression of Terrorist Financing Act No 25 of 2005**
- **Financial Transactions Reporting Act No 06 of 2006**
- **All gazettes, directions, circulars, instructions issued by the FIU from time to time**

ii. Predicated offences under the Prevention of Money Laundering Act

*Refer Annexure I of this Policy*

As per the Act, 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.

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.

1.4 **Powers of the 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 facilitate the prevention, detection, investigate and prosecute over the offences of money laundering and financing terrorism.

b) Under the powers vested by the Act, FIU can require institutions to undertake due diligence measures to combat money laundering and terrorist financing.

1 FIU powers listed above is only a summary and powers of FIU do not restrict to above only
c) FIU is empowered to carry out examinations of all institutions for the purpose of ensuring compliance with rules and regulations.

d) FIU is also 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.

2.0 AML and STF Program of the Bank

DFCC Bank attributes the highest importance to prevent the Bank from being utilized as a conduit and/or to be directly or indirectly be used for financial crime purposes by its customers. This Policy is a high-level guide and all stakeholders of the Bank need to be aware of the contents of same.

2.1 Applicability of Laws and Customer due Diligence Rules

i. All stakeholders of the Bank shall be guided by laws and regulations in respect of AML and STF.

ii. Bank shall take measures as specified in laws and any other Rules for the purpose of complying with following;

   a) Money Laundering and Terrorist Financing Risk Management of the Bank

   b) Customer Due Diligence for all customers and transactions. (Customers shall include regular account holders as well as Occasional Customers, One-off Customers, Walk-in-customers and Third Party Customers, legal Persons, Legal Arrangements and third parties, who are connected customers on transactions carried out with correspondent banks, wire transfers.)

2.2 Risk Based Approach on Customer Due Diligence

2.2.1 Critical elements on Risk Assessment

In terms of Extraordinary Gazette No 1951 /13 dated 27th January 2016 on Financial Institutions Customer Due Diligence Rules (CDD) No 01 of 2016, Bank shall be adopting “Risk Based Approach” (RBA) for the purpose of identifying, assessing and managing money laundering, terrorist financing risks pertaining to Bank. Bank’s RBA shall be proportionate to the nature, scale and complexity of the Bank’s activities, customer profile and money laundering, terrorist financing risk posed to the Bank on its day to day operations.

Business lines of the Bank shall primarily assess the AML/STF risk, when entering into and continuation of relationships, conducting transactions on criterions given below.

   i. Customers

   ii. Geographical areas

   iii. Products
2.2.2 Bank wide AML/STF risk assessment

Bank wide risk assessment based on above elements, will be carried out by Compliance Department. Appropriate risk assessment methods, risk matrixes, process and systems shall be develop 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 Board, annually.

Risk assessment report presented to the Board shall encompass the following at minimum,

i. Bank’s AML/STF exposure in terms criterions given in Section 2.2 above
ii. Findings and outcomes of the transaction monitoring
iii. Details of significant risks involved either internally or externally; modus operandi and its impact or potential impact on the Bank
iv. Recent developments in written laws on AML or STF
v. Details of Training programs conducted to mitigate the Money Laundering and Terrorist Financing risk on the bank

2.3 Responsibilities of the Board on AML/STF

Board shall;

i. Understand the legal regime and regulatory environment governing the Anti Money Laundering Laws and Suppression of Terrorist Financing.

ii. Approve internal policy of Anti Money Laundering and Suppression of Terrorist Financing.

iii. Ensure that Bank takes appropriate steps to identify, assess and manage its Money Laundering and Terrorist Financing Risks.

vi. 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/STF and rules.

v. Ensure that the Board receives timely reports of Bank’s risk assessment on money laundering and terrorist financing risk profile, effectiveness, risk control and mitigation measures.

vi. 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 STF.
vii. Maintain an independent audit function in order to effectively assess Bank’s internal policies, procedures and controls over AML and STF.

viii. Ensure the Compliance function is equipped with appropriate systems and resources.

2.4 Responsibilities of the Senior Management

i. 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.

ii. 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.

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

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

vi. 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

2.5 Responsibilities of the Compliance Officer

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 Suppression of Terrorist Financing Policy, which will include the following;

   (a) Customer identification requirements
   (b) Record keeping and retention requirements
   (c) Requirements for conducting ongoing due diligence on business relationships and ongoing scrutiny of transactions throughout the business relationship
(d) Reporting requirements including reporting of suspicious transactions and customer transactions.

(e) Ensure requirements of screening new staff before hiring them as employees.

(f) Keep staff informed of new regulations issued in relation to AML

(g) Conduct required staff training

(h) Monitoring of transactions

(i) Submission of regulatory returns

(j) Act as a Regulatory contact point

3.0 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 due diligence as the level of risk associated with the customer varies. For proven lower risk situations, simplified measures may be permitted to the extent given by CDD rules. Where the risks are higher, banks should take enhanced measures to mitigate and manage those risks.

Bank’s basic customer acceptance policy is set forth below. Detailed procedures relating to CDD shall be communicated as required time to time in respective manuals, guidelines and instructions.

i. 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.

ii. Bank shall not operate and maintain accounts where the ownership is transferable without the knowledge of the Bank.

iii. Bank shall not operate and maintain accounts where the account holders name is omitted.

iv. Bank shall maintain accounts and information in a way that assets and liabilities of a given customer can be readily retrieved.

v. Bank shall not maintain accounts separately from the Bank’s usual operational process, systems and procedures.

vi. Bank shall conduct CDD measures as specified in rules issued by FIU from time to time and any other appropriate guidelines that is proportionate to the nature, scale and complexity of Bank’s activities and ML and CFT risk profile.

vii. Bank shall not enter into relationship with certain business categories. Further, Bank shall conduct Enhanced Due Diligence when entering into relationship with High Risk Customer categories.
Refer Annex II of the Policy for Excluded and High Risk Customer Categories and EDD measures

viii. Beneficial owners, Legal Persons and Legal arrangements

If a relationship is being created for a customer who is not a natural person, Bank shall take reasonable steps to understand the ownership structure of the customer and determine the natural persons who ultimately own or control such customer.

Identification, verification, documents, delayed verification time lines and any other relevant steps that are required to be adopted in line with CDD rules on beneficial ownership should be complied.

ix. Continuous Customer Due Diligence

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 of a customer shall be conducted based on the below given periodicity.

<table>
<thead>
<tr>
<th>Customer Risk Category</th>
<th>CDD frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk</td>
<td>Annually</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>Every three years</td>
</tr>
<tr>
<td>Low Risk</td>
<td>Every Five years</td>
</tr>
</tbody>
</table>

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

Any transaction or series of linked transaction if exceeds two hundred thousand rupees or equivalent in foreign currency, conducted by any of the customers mentioned above, Bank shall conduct CDD measures and obtain copies of Identifications.

xi. 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.

xii. Customers and Financial Institutions from High Risk Countries

Bank shall apply enhanced due diligence measures to customers from high risk countries. Such countries will primarily be decided based on FATF listing, depending on other ML and FT scenarios unique to such countries and information through public domain. Compliance Department shall time to time issue instructions in this regard.
xiii. Politically Exposed Persons

Bank shall apply enhanced due diligence measures to Politically Exposed Persons. Officers are required to obtain prior approval from the Chief Executive Officer or in the absence of CEO from Deputy Chief Executive Officer or Chief Operations Officer before entering into relationship with PEPs.

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 CEO and in the absence of CEO from D/CEO or COO for continuation of the relationship.

xiv. Agency Functions of Money or Value Transfer Service Providers (MTV’S)

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.

Bank has to ensure that MTVS providers are guided by provisions of the CDD gazette in terms of wire transfers.

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.

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.

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.

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.

xv. 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 Compliance Officer.
Staff members responsible for correspondent bank relationships shall ensure that the Bank does not undertake business with shell financial institutions\(^2\) and ensure that no accounts for shell financial institutions are opened by the Bank.

### 4.0 Training and Awareness

#### 4.1 Responsibility on Staff Training and Awareness

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.

### 5.0 Risk Mitigating on Customer Transactions

It is imperative that bank has in place proper controls to mitigate the AML risk to the Bank at customer on boarding and transaction processing. In this regard bank has placed following controls to identify suspicious transactions and customers of negative records.

#### 5.1 Transaction Monitoring

i. Bank has established a transaction monitoring system (AML Software) to identify/track suspicious transactions and transaction trends to ascertain whether transactions are consistent and in line with the customers' known profile. Respective staff members are required to be well acquainted with the system.

ii. AML Software is based on a rule engine which has static rules inbuilt in order to generate alerts. These rules are based on various money laundering typologies experienced all over the world. During the end of the day process, all transactions in the core banking system will be processed through the AML software and any transaction which is violating the rules inbuilt will generate alerts. It should be noted the violation of a rule does not necessarily imply that it is money laundering transaction or a threat. It can 99% be a common transaction.

\(^2\)A **shell financial institution** is a financial institution that does not have a physical presence in any country.
Generation of an alert on a transaction is an indication that the transaction requires further clarifications.

iii. AML software also shall be used to risk rate customers in terms of CDD gazette.

5.2 Sanction Program

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

i. Any type of sanction that has been made into Law of the country or as issued as a directive by respective regulatory authority with specific authority to banks or that has an indirect compliance requirements
ii. Internationally Sanctioned Countries and Designated Persons by the United Nations
iii. Sanction Programs of Office of Foreign Assets Control (OFAC)
iv. Any other international sanctioned program that would have an impact on Correspondent Banking Relationships as decided by the Compliance Officer time to time

Refer Annexure III for details on customer screening

6.0 Reporting requirements for Suspicious Transactions

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

Refer annexure IV for examples of suspicious transactions

6.1 Suspicious transaction reporting procedure:

(I) If a staff member suspects or has reasonable grounds to suspect or has an honest belief that the funds or proceeds of an unlawful activity or related to terrorist financing, it should promptly informed and a suspicious transaction report (STR) should be 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.
6.2 Confidentiality and Non-disclosure

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

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

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

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

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

6.3 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.

6.4 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.

7.0 Record Retention

To assist the authorities when investigating cases of suspected money laundering, it is essential that evidence of customer identification, address verification and all transactions is retained for at least six years. Bank shall retain prescribed records of identification, pertaining to information gathered, mandates, and documents relating to transactions for a minimum of six years.
i. Following records /reports shall be retained for a period of at least six years after the relationship with the customer has ended.
   - Identification and account opening records
   - Documents verifying evidence of identity (including address)
   - Non-account holders identifications
   - Account transaction records
   - Every transaction undertaken for a customer
   - Records relating to training internal and external,
   - Records of compliance monitoring of transactions
   - Suspicious Transaction Reports
   - Documentary evidence of any action taken in response to internal and external reports of suspicious transactions
   - Mandatory transaction Reports (CTR, EFT – In and Out)

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

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

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

This policy shall be reviewed on annually.
Annexure 1

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;
h) Offences under any law for the time being in force relating to cyber crime;
i) Offences under any law for the time being in force relating to offence against children
j) Offences under any law for the time being in force relating to offences connected with the trafficking of persons; and
k) Offences under any other law for the time being in force which is punishable by death or with imprisonment for a term of five years or more.
Annexure II

1.0 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.

2.0 High Risk Customer Categories
Following types of customer categories shall principally be treated as High Risk and respective Branch Managers / Relationship Managers 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
   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 individuals
   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

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.

3.0 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
Annexure III

Bank’s Sanction Program will consist of;

i. AML Software

ii. On line licenses and Batch uploads

iii. On line Licenses Manual Process

Bank will in principle screen following categories before entering into relationships and during the relationships on a periodic basis.

i. Customers when entering into any relationship including (not limited) following
   - Accounts
   - Virtual Wallets
   - Credit cards
   - Remittance payments (Ex; Western Union, Lanka Money Transfer System (LMT))
   - Correspondent Banks

ii. Trade transactions prior to effecting a transaction

iii. All inward remittances

iv. Batch processed transactions different transaction modules, products such as Exchange House Remittances, Lanka Money Transfer system

v. Customer Transaction level screening

vi. Customer Base Periodic Checking

vii. Service Providers, Agents, Outsourced Service Providers

viii. Major Shareholders

ix. Related Parties, Key Management Personnel, all other employee categories
Annexure IV

Examples for suspicious transactions

- 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
- Transactions in which assets are withdrawn immediately after being deposited, unless the customer’s business activities furnish a plausible reason for immediate withdrawal
- 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
- Frequent withdrawal of large cash amounts that do not appear to be justified by the customer’s business activity
- Large cash withdrawals from a previously dormant/inactive account or from an account which has just received an unexpected large credit from abroad
- Frequent address changes by customers/clients
- Client does not want correspondence sent to home address.
- 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.
- Unusual nervousness of the person conducting the transaction
- Client insists on a transaction being done quickly.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client attempts to convince employee not to complete any documentation required for the transaction.
- Large contracts or transactions with apparently unrelated third parties, particularly from abroad
- Extensive and unnecessary foreign travel