October 2018	Anti-Money Laundering & Combating Financing of Terrorism Policy

Compliance and *Internal Control Division*

Contents

1. Introduction

Money laundering is the process by which the proceeds derived from illegal activities are so channelized that its source and origin is concealed behind multiple layers. The money laundering covers wide range of activities but generally there are three common stages in the process;

Placement: The introduction of illegally obtained monies or other valuables into financial or non-financial institutions.

Layering: Separating the proceeds of criminal activities from their source through the use of layers of complex financial transactions (domestic and/or cross border). These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

Integration: Placing of laundered proceeds back into the economy in such a way that they re-enter the financial system, apparently, as legitimate funds.

The above stages are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process.

In law (AML Act 2010), in addition to the offender, a person is also considered guilty of offence of money laundering who participates in, conspires/attempts to commit, facilitates or counsel the commission of the acts of money laundering process, knowing or having reason to believe that such property is proceeds of crime. The offence is punishable with rigorous imprisonment from one to ten years with fine up to one million (five million in case of a company) and forfeiture of the property involved.

Terrorism and Terrorist Financing

Terrorism can be defined as the criminal acts intended or calculated to provoke a state of terror in the general public for whatever the considerations may be; political, ideological, racial and religious or any other nature that may be invoked to justify them. The financing of terrorism is the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism.

Terrorist financing refers to accommodating or facilitating financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/or terrorist organizations. Once the financial institution knows or suspects, or should reasonably suspect that an individual/group is associated with any terrorist activity or group, a financial institution (in carrying out a transaction for or with that individual/group), may be considered as facilitating terrorist activity whether or not the institution knows the specific nature of the activity facilitated, or whether any terrorist activity was actually carried out.

The two activities, money laundering and financing terrorism, are linked because the techniques used to launder money are essentially the same as those employed to conceal the sources and uses

of terrorist financing. However, there are two major differences between the use of terrorist and criminal funds:

- Often only small amount are required to commit a terrorist activity.
- Terrorism can be funded from legitimately obtained income, including charitable donations. This process is also known as reverse money laundering.

2. Purpose

The Bank is committed to the highest standards of Anti-Money Laundering (the "AML") compliance to prevent use of its products and services for money laundering purposes. These standards also set out the basic framework for Combating Financing of Terrorism (CFT) i.e. to detect, prevent and suppress the financing of terrorism and terrorist acts. This policy establishes standards for maintaining an effective AML/CFT program protecting BOP, its employees and clients from being misused for money laundering, terrorist financing or other financial crimes.

3. Scope

The standards set out in this policy are minimum requirements based on applicable legal and regulatory requirements and apply to:

- All business/functions and employees (Permanent, contractual or outsourced)
- New products, services, business practices, including new delivery mechanisms
- New and existing business relationships, including walk-in customers
- Customer related transactions.

4. The Bank's Policy

It is the policy of the Bank:

- To ensure that statutory and regulatory requirements of AML and CFT regulations are complied with.
- To mitigate the risk of Bank's services including wire transfer and products being abused for the purposes of money laundering and terrorism financing.
- To define a mechanism to accept a new relationship to minimize the Bank's risk.
- Effective Customer Due Diligence and ongoing monitoring thereof.

- Cash transactions for non-account holders of the Bank are monitored and will be subject to additional controls that include identifying and verifying the identity of walk- in customers conducting transactions above the limit prescribed by the Bank.

- Established relationships are regularly monitored, to ensure that they fit the customer's profile, especially in respect of abnormal or out of pattern transactions.

- Reporting of CTR (Currency Transaction Report) & STR (Suspicion Transactions Report) to Financial Monitoring Unit (FRMU) as per AML Act, 2010.

- Maintenance of records to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations, if required.

- Adequately train Bank's staff to implement AML/CFT policy effectively.

5. Responsibilities

According to AML Act, 2010, a person is also considered guilty of offence of money laundering who participates in, conspires/ attempts to commit, facilitates or counsels the commission of the acts of money laundering process, knowing or having reason to believe that such property is proceeds of crime. The offence is punishable with rigorous imprisonment, fine and forfeiture of property involved. Accordingly, nobody should set out to offer product or services or provide active assistance in transactions, which in their opinion, are associated with money derived from/for illegal activities. It all can start from the account opening / on boarding process where it is mandatory to identify beneficial owner / true owner along with identification and validation of source of funds.

5.1. Board of Directors

The Board shall ensure that the Bank shall formulate and put in place, a comprehensive AML/CFT policy and ensures its implementation and periodical review as per frequency defined in this Policy.

The Board may delegate these tasks to one of its sub-committees; Central Audit Committee or Board Risk Management Committee, or both.

5.2. Management

The Management is responsible for effective management of the Bank's money laundering and terrorism financing risks through AML/CFT policy and procedures. The line function shall be responsible for day to day compliance with anti-money laundering and terrorist financing obligations within all segments of the Bank for which they are responsible.

Monitoring of compliance and AML-CFT functions are part of TORs of Compliance Committee, who shall ensure that bank's AML/CFT risk is properly managed.

In order to strengthen the AML-CFT culture of the bank, compliance related to AML /CFT responsibilities shall be included in the key performance indicators (KPIs) of the staff responsible down the line. Moreover, RMG shall ensure that ML/TF risk shall be included in the KPIs of officer responsible for Enterprise Risk Management and Operational Risk Management functions.

5.3. Compliance & Internal Control Division

Anti Money Laundering Officer (AMLO) appointed by the management for the Bank will primarily be responsible for the following:

- To review compliance with AML statutory and regulatory obligations, in respect of the Bank's Anti-money laundering policy and periodic reporting to Senior Management.
- Advising Senior Management of any deviations from the Bank's policies and procedures that have been noted by C&ICD.
- Ensure that AML/CFT Policy is updated with changes in regulations and communicated to all concerned.
- Effective implementation of AML/CFT program
- To track changes in the statute and other promulgations affecting AML/CFT Policy for facilitating periodical review as per the frequency defined in this Policy and arranging approval from the BoD.
- To improve/align Risk Based Approach (Customer Risk Assessment) and AML/CFT risk assessment procedures in line with SBP guidelines.

Head C&ICD has the authority and powers to access all bank's record related to core system information, MIS, physical files, loan / advances, trade related data, Account opening Registers, vouchers etc.

5.4. All Employees at Business/Branches

Everyone involved in the process of establishing business relationship and conducting transactions including wire transfers must familiarize themselves with this policy. A comprehensive training program is being conducted for front end staff to ensure that they have necessary knowledge on the subject. Employees are also encouraged to raise and escalate queries in case they need guidance or assistance from Compliance Function. Business Units, departments and branches shall strictly adhere to this policy, AML/CFT program and standard operating procedures to carry out their specific duties to prevent use of products and services for the purpose of money laundering and terrorism financing. All employees are responsible for:

- Remaining vigilant to the possibility of money laundering and terrorist financing.

- Complying fully with all anti money laundering procedures in respect of customer identification, verification of the source of the funds, account monitoring, record keeping and reporting.

- Reporting all suspicions of money laundering and terrorism financing to the C&ICD.

- Employees who violate any provision of the AML Act, 2010 or under this policy will be subject to disciplinary action.

5.5. Internal Audit Function

In addition to Compliance own reviews, Audit & RAR Group shall report non-compliances of AML/CFT Policy to respective line management along with its copy to Head C&ICD to ensure rectification of exceptions observed during their audit.

6. AML/CFT Program

Adherence to AML/CFT program is responsibility of all employees of the Bank. The program includes:

1. Client Acceptance Policy
2. New Products/Services/Business Practices
3. Customer Due Diligence (CDD)
4. Wire Transfer
5. Reporting of currency/suspicious transactions to competent authority
6. Threshold Limits
7. Training
8. Record Retention.

6.1. Client Acceptance Policy

6.1.1. Client Acceptance

The branches/business must exercise prudence and vigilance while establishing a new business relationship. To safeguard against the risks of money laundering and financing terrorism, the business relationship must be established after ensuring that account documentation is complete and CDD measures are conducted satisfactorily. The CDD measures shall also apply when conducting transactions for Occasional/Walk-in customers. No relationship shall be established

until beneficial owner and source of funds are established. Business shall determine beneficial ownership and would screen it from all the available negative list.

In case the branches are not able to satisfactorily complete CDD measures, including identity, beneficial ownership or information on purpose and intended nature of business relationship, account should not be opened nor any service provided. Consideration shall be given if the circumstances are suspicious so as to warrant the filing of Suspicious Transaction Report (STR).

6.1.2. Anonymous or Fictitious Account

BOP shall not open and maintain anonymous accounts or accounts in the name of fictitious persons or with beneficial ownership other than account holder.

6.1.3. Services to Proscribed Entities and their Associates

BOP shall not provide any banking services to proscribed entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed name or with a different name. All accounts must be screened properly without exceptions and Bank has zero tolerance policy in this regard. Account opening officer shall ensure that account is properly screened through Compliance Link. All home remittance transactions shall be screened by Branches before payment over the counter.

6.1.4. High Risk Customers

During CDD process the branches/business may come across certain types of customers that pose higher than the average risk due to their background, country of origin, public or high profile position, nature of business etc. In such a case, they must undertake Enhanced Due Diligence (EDD) and obtain higher management's approval before establishing a relationship. Following types of relationships are considered relatively high risk:

- Non-Governmental Organizations (NGOs), Not-for-Profit Organizations (NPOs), Charities, Trusts, Clubs, Societies, Associations & Exchange companies etc.
- Politically Exposed Persons
- Correspondent Banking
- On-line services and issuance of remittance instruments to occasional/walk-in customers
- Customers in cash intensive business, frequent wire transfers or users of locker facility
- Certain geographic locations are more vulnerable to money laundering, terrorist financing and other crimes e.g. jurisdictions indicated by Financial Action Task Force (FATF) for non-cooperating or not applying its recommendations.

- Relationship with existing customer shall be treated as high risk if any account is not conducted to the satisfaction of the Bank in line with this policy.

- Accounts of NGOs, NPOs, Charities, Trusts, Clubs, Societies, Associations & Exchange companies, Politically Exposed Persons and Correspondent Banking shall be approved by the Compliance Function of the Bank.

6.1.4.1. NGOs, NPOs & Charities

The branches shall conduct EDD while establishing relationship with NGOs, NPOs and Charities to ensure that these accounts are used for legitimate purposes and the transactions are commensurate with the stated objectives and purposes. The accounts should be opened in the name of relevant NGO, NPO & Charities as per title given in its constituent documents of the entity. Comprehensive CDD of the individuals who are authorized to operate these accounts and members of their governing body shall be conducted to ensure that these persons are not affiliated with any proscribed entity, whether under the same name or a different name. Caution shall be marked on accounts soliciting donations in its account through advertising in newspapers or any other medium by mentioning a different title of the account and STR may be filed, where required.

6.1.4.2. Politically Exposed Persons

Politically Exposed Persons (PEPs) means natural persons who have been entrusted with prominent public functions either domestically or by a foreign country, or in an international organization whose substantial or complex financial or business transactions may represent an enhanced money laundering or terrorist financing risks. This includes Heads of State or government, senior government, juridical or military officials, senior executives of government owned corporations/department/autonomous bodies, senior politicians, important political party officials, etc., and their family members or close associates. Asset side due diligence of all PEP accounts in case of borrowing relationship shall be done by RMG, while Credit Approvals will be granted with the concurrence of CEO irrespective of exposure amount and relevant approving authority, whereas account opening shall be allowed / approved by Compliance Function.

6.1.4.3. Correspondent Banking

Correspondent banking is the service by which one bank provides services to another bank to open and maintain accounts in different currencies, fund transfers, cheque clearing or carry out variety of other transactions.

Correspondent banking relationships present unique risks to which the management must pay close attention, due to concerns with respect to the difficulty of performing any due diligence or monitoring of the other bank's customers. Attention must be paid to the transparency of ownership, banking licenses, their AML/CFT policies, sanctions/embargoes and Advisories about risks, effectiveness of their regulatory bodies, their correspondent accounts servicing foreign financial institutions (non-banks) such as money changers, shell banks etc. Ensure relationship or

transactions with counterpart from or in countries which sufficiently apply recommendations of FATF.

All correspondent banking relationships shall be approved by the senior management including Compliance Function. C&ICD shall review CDD / EDD of correspondent relationship on a predefined frequency.

In case the BOP is availing correspondent banking services from a bank/financial institution abroad, the CDD measures shall be applied, as considered necessary to mitigate Money Laundering / Terrorism Financing risks. . BOP shall not establish any relationship with the banks that appears on the sanctioned lists or have any negative media repute.

6.1.4.4. Shell Banks

It is prohibited to have a relationship with a correspondent bank that is a shell bank, or a bank that permits its accounts to be used by shell banks. A shell bank means a financial institution incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management and which is not affiliated with a regulated financial group.

6.1.4.5. Enhanced Due Diligence

Besides approval from senior management, branches/business shall conduct Enhanced Due Diligence (EDD) for establishing relationship with high risk customers. EDD shall include:

- Obtaining additional information on customer's (including beneficial owner, if any), intended nature of business, source of funds/wealth and need of certain products & services like intense cash transactions or frequent wire transfers including bank's own assessment to this effect .

- Increased monitoring of customers' accounts and updating their profile periodically at a reduced interval in comparison with low or medium risk customers.

6.1.4.6 Government Accounts

Government accounts shall not be opened in the personal names of the government official(s) and all KYC formalities shall be properly completed. A government account which is to be operated by an officer of the Federal/Provincial/Local Government in his/her official capacity, shall be opened only on production of a special resolution/authority from the concerned administrative department duly endorsed by the Ministry of Finance or Finance Department of the concerned Government.

However, in case of autonomous entities and Armed Forces including their allied offices, bank accounts may be opened on the basis of special resolution/authority from the concerned administrative department or highest executive committee / management committee of that entity

duly endorsed by their respective Unit of Finance. Rules, regulations or procedures prescribed in governing laws of such entities relating to opening and maintaining of their bank accounts shall also be meticulously complied.

Foreign currency accounts of Government, Semi Government, Autonomous bodies and Public Sector Entities shall only be opened if these accounts comply with Foreign Exchange regulations of SBP and have proper purpose along with prior approval of SBP.

6.1.4.7. Personal Accounts for Business, Donations and Other Purposes

Personal accounts shall not be used for business purposes. In case of unsatisfactory transactions the Bank through C&ICD may consider it for reporting it to Financial Monitoring Unit (FMU) and / or may close the account. Asaan account shall strictly be operated as per criteria set by SBP.

Personal accounts shall not be allowed to be used for charity purposes/collection of donations.

6.1.4.8. Screening of Customers through proscribed lists

New Relationships: All new relationships shall be subject to comprehensive screening through application (Accuity's Compliance Link- Automated Screening Manager). The name of the individual, attorney, trustee or beneficial owner must be screened through Compliance Link utility. Following lists have been activated in the system;

Global Watch List: US-OFAC (Office of Foreign Assets Control), UNSC (United Nation Security Council), BofE (Bank of England), EU (European Union), and HMT (Her Majesty's Treasury).

Local Lists: 4th Schedule ATA (Anti-Terrorism Act) 1997, NAB (National Accountability Bureau) & local PEP lists.

Batch Screening: Batch screening of all existing portfolio shall be conducted on annual basis through Compliance Link utility and in case any true match is found relationship shall immediately be terminated and considerations shall be made regarding filing of STR. The activity shall be dependent on availability of data from IT Division.

Likewise, all occasional / walk-in-customers receiving home remittance payments over the counter or purchasing any remittance instruments shall also be screened through this utility. No product or services shall be offered to individual/entity whose name appear in Global Watch List & 4th Schedule ATA List however, for customer appearing on the NAB list, attention must be paid before extending any financing facilities and branches must conduct EDD including senior management approval for such customers to establish their true identity and use of funds.

6.2. New Products/Services/Business Practices

The development of new products, services and business practices, including new delivery mechanism must follow the process outlined in the Other Risk Assessment Procedure (ORAP). SBP's prior concurrence is obtained if it involves regulatory issues. The Compliance Function must be involved in the process to ensure that customers are identified, verified and the financial transactions in which they engage are monitored to mitigate the risks of money laundering and terrorist financing.

6.3. Customer Due Diligence

Apply Customer Due Diligence (CDD) measures, including identifying and verifying the identity of the customers when:

- Establishing business relationship
- Conducting occasional transactions
- Carrying out occasional wire transfers (domestic/cross border)
- There is suspicion of money laundering/terrorist financing.

Customer Due Diligence Measures

The CDD processes consist of the following:

1. Identification of customers
2. Verification of identity
3. Obtaining Information on the purpose and intended nature of business relations
4. Customer risk assessment
5. Conducting Ongoing Due Diligence on the business relationship and scrutiny of transactions undertaken throughout the course of relationship.
6. In case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them were individual customers of the Bank.
7. Proper justification shall be recorded for opening of multiple accounts within same or different branches of the Bank.

Note: The Bank shall conduct comprehensive CDD of the individuals who are authorized to operate the accounts of NGOs, NPOs and Charities, and members of their governing body.

Due Diligence Measures for Borrowers / Assets Side Customer

RMG shall make comprehensive due diligence on asset products and related customers to ensure effective implementation of AML/CFT requirements. This shall include monitoring purpose of loans and related risks on ongoing basis as per standard norms and best practices to mitigate the risks related to such products / customers with AML perspective.

6.3.1. Identification of Customers

Every customer must be identified for establishing a business relationship. For the purpose, the branches must obtain minimum set of documents to identify natural as well as legal persons, NGOs, NPOs, charities, trusts or legal arrangements etc. as prescribed by the SBP. This includes identification of natural person(s) acting on behalf of customer or where customer is legal person and the 'Beneficial Owner'.

6.3.1.1. Beneficial Owner

A beneficial owner means:

- The natural person who ultimately, directly or indirectly, owns or controls a customer.
- The person on whose behalf a transaction is being conducted.
- The person who exercises ultimate effective control over a person or a body of persons whether incorporated or not.

Where the customer is not a natural person, reasonable measures be undertaken to understand ownership and control structure of the customer to determine the natural persons who ultimately own or control the customer.

6.3.2. Verification of Identity

The identities of the customers (natural persons) and in case of legal persons, identities of their natural persons, person acting on behalf of customer and beneficial owner must be verified from relevant authorities/documents issuing bodies and where necessary using other reliable, independent sources and retain copies of all reference documents used for identification and verification. The verification shall be completed before business relations are established including verification of CNIC/NICOP/POC/SNIC from NADRA in case of new customers. The verification shall be the responsibility of the Bank for which the customer should neither be obligated nor the cost of such verification be passed on to the customers.

CNIC/NICOP/SNIC of natural persons whether individuals, sole proprietors, partners, directors, trustees, beneficial owner etc. must invariably be verified from NADRA before opening of the account. For this purpose, all individuals (natural persons) and authorized signatories in case of entity account shall be verified biometrically being a regulatory requirement. For cases where

biometric verification cannot be done temporarily due to genuine reason or technical issues, as explained below:

a) NADRA system/data/connectivity or technical issue beyond a reasonable time

b) NADRA does not have biometric records of prospective customers

c) Customers whose eligible identity documents are other than biometrically verifiable documents, e.g. Passport, Alien Registration Card, etc.

d) Customer's permanent physical disability, e.g. limbs disability, uneven texture/ erased / unclear fingerprints, etc.

e) Customer's temporary issue e.g. wounded/ bandaged hands/ mehndi, etc.

In above cases, NADRA Verisys of the customer shall be conducted with proper reasoning and proof, however biometric verification shall still be required once the above issue is resolved. No relaxation beyond above points/ conditions given by SBP for Biometric verification shall be allowed.

Branch management shall obtain prior approval from line management (at least one step high) / C&ICD for completing verification of other constituent documents as prescribed by State Bank in AML/CFT Regulations (Annexure 1), including employer's certificate in case of a salaried person, Passport of a foreign national, verification of documents for CNIC which does not contain a photograph, photo of an individual with shaky signatures etc. However, no debit will be allowed or cheque book is issued until positive verification is completed. The branch shall report completeness of verification and seek approval of the approving authority to activate the account operation.

In case of negative verification, the branch must refer it to the line management to decide filing an STR if circumstances are suspicious or whether relationship is needed to be closed. In the latter case, amount collected may be returned through a payment order clearly mentioning the reason "Account closed; unable to verify identity document".

Account opening and approving officer / Business Group shall be responsible for monitoring of deferrals (if any) allowed on SBP criteria to ensure biometric verification of identity is completed within the prescribed time.

Branches shall maintain complete record of customers / deposits;

i) Where business relationship was refused or terminated on account of negative verification or inappropriate risk rating.

ii) Account opening cases rejected by Compliance and Central Processing Unit

iii) Account closed on Money Laundering / Terrorist Financing Risk.

In order to further verify the genuineness, a 'Letter of Thanks' shall invariably be dispatched to every new relationship at the address provided for correspondence through the couriers. It may also be dispatched through Registered A.D. Post, where courier services are not available. The cheque book shall not be issued in cases where the letter is returned undelivered till complete satisfaction of the branch management regarding customer's address. A copy of letter of thanks brought back by the customer duly signed by him must be kept on record before account activation or cheque book issuance.

6.3.3. Obtaining Information on the Purpose and Intended Nature of Business Relations

All branches must obtain information, from new customers, as to purpose and intended nature of business relations with BOP, specifically if they intend to have borrowing relationship and EDD for all such customers shall be performed.

6.3.4. Customer Risk Assessment

The bank shall procure and install / implement a suitable KYC application to automate risk assessment and connected with existing portal to achieve integration across the bank. The branches/ business shall apply risk based approach and calculate the customer risk to identify risks of money laundering and terrorist financing associated with a prospective relationship. Risk based approach allows for the possibility to use different measures in different situations and risk levels (low, medium or high), depending on;

- The client or client segmentation
- Categories
- Geographies (Country of residence / correspondence)
- Source of wealth
- Type and method of account
- Screening through proscribed list
- Negative media repute
- product and service needs

All high risk relationships (Accounts of NGOs, NPOs, Charities, Trusts, Clubs, Societies, Associations & Exchange companies, Politically Exposed Persons and Correspondent Banking) shall be approved Senior Management i.e not below the rank of Executive Vice President as designated by the Board for the purpose of AML/CFT regulations.

Whereas reduced or simplified CDD/KYC measures shall be applied where risks are low such as Asaan account and information on the identity of the customer and the beneficial owner is publicly available or here adequate checks and controls exist to mitigate money laundering and terrorist financing.

Customer risk assessment is a regulatory requirement, no customer account shall be opened without risk assessment.

6.3.5. CDD for Occasional/Walk-in Customers

6.3.5.1. Cash Transactions

Obtain copy of identity document from occasional/walk-in customer conducting cash transactions up to threshold limit fixed by State Bank of Pakistan(varies from time to time) whether carried out in a single operation or in multiple operations that appeared to be linked. For unusual transaction, these customers can be verified through Biosys or Verisys.

6.3.5.2 On-line transactions

Obtain a copy of CNIC (regardless of threshold) while conducting online transactions by occasional customers/walk-in-customers (except deposits through Cash deposit machines or cash collection/management services). Originator's information/particulars shall be captured in the system and made accessible along with transaction details at beneficiary's branch for transaction exceeding a certain threshold limit as prescribed by State Bank of Pakistan from time to time.

Branches are advised to do necessary check such as Biosys or Verisys on identity for unusual transaction along with a preliminary query on source of funds and purpose of remittance. Same is also applicable in case of remittance instruments.

6.3.5.3 Remittance Instruments

Obtain copy of identity document issued by NADRA from each occasional/walk-in customer who wish to purchase remittance instrument e.g. POs, DDs, MTs etc.

6.3.6 Ongoing Monitoring and Due Diligence

6.3.6.1 Transaction Monitoring

All transactions are monitored on an ongoing basis to ensure that the transactions are consistent with the Bank's knowledge of the customer profile. Account threshold must be set by Branches and reviewed by CPU with documents reflecting profile & source of funds of the customer.

The background and purpose of complex, large value transactions and unusual pattern of transactions which have no apparent economic or visible or lawful purpose shall be inquired, examined and findings be documented. Customers' profiles should be revised keeping in view the

spirit of KYC/CDD and basis of revision shall be documented and customers may be consulted, if necessary. Revised KYC must be kept on record. Threshold revision must be allowed only after proper documentation or other information to be available on record and approved by relevant approving authority. CPU will review the Branch request and will make necessary changes accordingly.

All existing relationships of NGOs/NPOs/Charities should be carefully monitored to ensure that these organizations, their authorized signatories, members of their governing body and the beneficial owners are not linked with any proscribed entities and persons, whether under the same name or a different name. In case of any positive match, the Bank may consider to file STR with SBP and take other actions as per law.

The Bank shall implement system to generate auto alerts for out of pattern transactions based on pre-defined parameters / thresholds for analysis and reporting of possible suspicious transactions. The Bank shall established criteria in AML/CFT procedures for management of such alerts.

For existing customers who has opened accounts with old NICs, the Bank shall ensure that attested copies of CNICs shall be obtained. The Bank shall block accounts without CNIC after serving one month prior notice for all debit transactions/withdrawals, irrespective of mode of payment, until the subject mandatory requirement is fulfilled. However, debit block from the accounts shall be revoked upon obtaining of attested copy of CNIC and biometric verification of the same from NADRA.

6.3.6.2 On-Going Due Diligence

Bank shall procure KYC tool to auto generate periodical review alerts and incase of any material change in KYC profile of the customer for analysis.

Following minimum frequencies would be followed according to risk assessment of account holders:

- High Risk : 12 Months
- Medium Risk : 18 Months
- Low risk : 24 Months

Ongoing due diligence of customers shall be conducted including but not limited to following factors:

- Material change in account operation like introduction of a new director, partner, attorney to operate account, change of account type or category, change of address, change of citizenship etc.
- Negative references in the sanctions lists or press/electronic media on the client's reputation.

- Change of status or particulars.
- Frequent use of lockers.
- Any other reason like declining of relationship from any other bank.

On the basis of ODD/periodic review branches shall update the CDD profile of the customer including EDD and shall seek approval from authority if required. KYC profile must also be updated on receipt of any adverse information / media report regarding customer profile.

If CDD of an existing customer is found unsatisfactory during ongoing review, the same should be immediately reported to designated officer of C&ICD for onward submission to FMU and other actions should be taken as per directions from the line management.

6.3.6.3 Dormant accounts

For customers whose accounts are dormant or in-operative, credit entries may be allowed without changing status of such accounts. However, Debit transactions/ withdrawals shall be allowed upon;

i. The request of account holder for activation along with afresh attested copy of CNIC if already not available.

ii. The biometric verification of individual / authorized signatory(ies) in case of entities

iii. Completion of CDD formalities including SOF (source of fund) and other necessary documents.

However, transactions such as debits under the recovery of loans and mark-up etc. any permissible charges, government duties or levies and instruction issued under any law or from the court will not be subject to debit or withdrawal restriction.

6.4. Wire Transfer

Wire transfer is the primary tool at all stages of money laundering process, but particularly in 'layering' operations. Accordingly, the branches shall;

Identify and verify the originator (whether domestic or cross border wire transfer irrespective of the amount) and obtain details of beneficial owner(s) of funds:

- Record complete details of the wire transfer so as to permit its reconstruction.
- Include originator's name, address, CNIC/Passport number and account number (or unique reference number which permits traceability of the transaction)
- Adopt risk based procedures for identifying and handling incoming wire transfers that are not accompanied by complete originator information.

- See with suspicion, the incoming wire transfers with incomplete originator information which may require reporting to FMU or termination of the transaction.

If the Originator information is accompanied along with payment message then the transaction shall not be passed through the system. The Bank would consider limiting or terminating relationship with financial institutions that do not comply with regulatory and statutory requirements of AML and CFT.

Bank has placed a screening tool (SWIFT Sanction Screening) for screening of all inward/outward Message Type (MTs) through sanctioned lists of individuals, companies, vessels & countries i.e. OFAC, UN, EU, BOE etc.

6.5. Reporting of Currency/Suspicious Transactions

The AML Act, 2010 requires the banks to:

- Report suspicious transaction, including attempted transactions, regardless of the amount of transaction to FMU.
- File Suspicious Transaction Reporting (STR), if the Bank knows, suspects or has a reason to suspect that the transaction:
    - Involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime.
    - Has no apparent lawful purpose after examining the available facts, including the background and possible purpose of the transaction.
    - Involves financing of terrorism.
- Justification for filing / not filing of STR shall be documented and placed on record.
- STR shall be filed with FMU immediately but not later than seven working days after forming the suspicion.
- Currency Transaction Report (CTR) shall be filed to the extent and manner prescribed by FMU. (Presently cash transaction amounting to Rs.2.0 million and above are reported to FMU).

Anti-Narcotics Force (ANF) being a premier Law Enforcing Agency to eradicate menace of narcotics trace and freeze assets of drug baron/suspects. Since amount lying in accounts/lockers is suspected to be accumulated through drug proceeds, analysis/findings must be reported to FMU as well as a written confirmation to this effect should also be forwarded to ANF. Before implementing de-freezing orders passed by the Trial Courts, clarifications MUST be sought from Law Department.

The willful non-compliance of STR filing or giving false information is punishable with imprisonment for a term which may extend to three years or fine up to one hundred thousand rupees and forfeiture of property involved in money laundering. Therefore all employees are advised to remain vigilent and highlight any / all unusual transaction(s) and refrain from opening of Accounts on which they are fully well versed profile and business of the party.

Accordingly, all branches must ensure that the transactions which are out of character or are inconsistent with the history, pattern, or normal operations of the account including heavy deposits, withdrawals and transfers, shall be viewed with suspicion, properly investigated and referred to Head C&ICD for possible reporting to FMU under AML Act, 2010.

The Bank, without disclosing the contents of STRs, shall submit to BPRD, State Bank of Pakistan on bi-annual basis a status report (indicating only No. of STRs s reported to FMU) within seven days of close of each half year.

All personnel are strictly prohibited from disclosing the facts to the customer or any irrelevant quarter that a suspicious transaction/ currency transaction or related information is being reported for investigation. The violation is a criminal offence punishable by a maximum term of three years imprisonment or a fine which may extend to five hundred thousand rupees or both.

6.6 Trade Based Money Laundering:

The term trade-based money laundering and terrorist financing (TBML/FT) refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origins or finance their activities. TBML/FT may be carried out includes, but are not limited to: misrepresentation of the price, quantity or quality of imports or exports; and money laundering through fictitious trade activities and/or through front companies.

TBML schemes may involve:

- Over or under invoicing: Misrepresenting the price of the goods.
- Multiple invoicing: Invoicing one shipment several times.
- Short or over shipping: Shipping more or less goods than invoiced.
- Obfuscation: Shipping something other than what is invoiced.
- Phantom shipping: Shipping nothing at all with false invoices.
- There are other types of TBML that do not fit neatly into categories of trade description fraud, such as related party transactions and the acquisition and sale of intangibles.

To combat TBML related risk following measures shall be adopted Bank wide to mitigate the risk to an acceptable level:

- Placing adequate controls, procedures and systems for preventing and managing the risks associated with trade finance activities, including effectively identifying and monitoring its trade finance portfolio for suspicious or unusual activities.

- Conducting risk assessment of customers via techniques such as Know Your Client/Customer (KYC) and Enhanced Due Diligence (EDD).

- Assessing and placement of TBML Red Flags and monitoring thereof.

- Be proactive in discussing TBML issues at all level including reporting suspicious activities/transactions to relevant authorities.

- Seek additional independent, reliable sources to verify information provided by the client, whereas suspicion of TBML arise.

- Check of shipping companies if suspicion related to shipment of goods is identified.

- Conduct customer onsite visit and re-examine their business records for higher risk trade products.

- Monitor customer's account activities periodically to ensure that transaction turnover commensurate with the business profile.

- Provide regular training to the staff as how to recognize and deal with transactions and other activities that may be related to money laundering.

- Reporting of suspicious transaction to FMU through C&ICD.

6.7 Threshold Limits

Business shall assign appropriate threshold limits in customer accounts and review them periodically. This is essential for effective monitoring of transactions at compliance level.

6.8. Training

For effective implementation of this AML/CFT policy as well as the regulatory requirements, HRD shall assess and design suitable training program in coordination with C&ICD for employees responsible for carrying out transactions and/or establishing business relationships every year. The training shall enable them to understand:

- New developments, money laundering and financing of terrorism techniques, methods and trends.

- Responsibilities relating to AML/CFT especially requirements relating to CDD.

- Analysis of abnormal or out of pattern transactions and alerts generated thereof for possible reporting of suspicious transactions.

L&DC / HRD shall ensure that respective directives from regulatory bodies are covered in these training sessions, including computer-based/online Training Program and testing awareness of the relevant staff on periodic basis disseminated through C&ICD.

6.9. Record Retention

Complete record of transactions (including reporting of Suspicious Transactions), domestic, or international, shall be maintained for a minimum period of ten years from completion of the transaction. The record so maintained should be sufficient to re-construct individual transactions.

The identification data obtained through CDD/KYC process, account files and business correspondence shall be retained for a period as prescribed by SBP after the business relationship is ended. The Bank shall retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority.