

Definitions:

Part-2: Customer Due Diligence and Anti Money Laundering (M)

- a. **“Beneficial Owner”** refers to the natural person(s) who ultimately owns or controls a customer and /or the natural person on whose behalf a transaction is being conducted and includes the person(s) who exercise(s) ultimate effective control over a person or a body of persons whether incorporated or not;
- b. **“Beneficiary”** means the person (natural or legal) to whom or for whose benefit the funds are sent or deposited in bank;
- c. **“Beneficiary institution”** means the financial institution that receives the funds on behalf of the wire transfer or electronic fund transfer beneficiary;
- d. **“Control”** in relation to a legal person, means the power to exercise a controlling influence over the management or the policies of the undertaking, and, in relation to shares, means the power to exercise a controlling influence over the voting power attached to such shares;
- e. **“Correspondent Bank”** means the MFB in Pakistan which provides correspondent banking services to bank or financial institution situated abroad and vice versa;
- f. **“Correspondent Banking”** means provision of banking services by one bank (correspondent) to another bank (respondent) including but not limited to opening and maintaining accounts, fund transfers, cheque clearing, payable through accounts, permissible foreign exchange services or similar other banking services;
- g. **“Currency Transaction Report”** means as defined under AML Act 2010;
- h. **“Customer”** means a person having relationship with the MFB which includes but not limited to holding of deposit/deposit certificate/ or any instrument representing deposit/placing of money with a MFB, availing other financial services, locker facility, safe deposit facility, or custodial services from the MFB;
- i. **“Customer Due Diligence or CDD”** in broader terms includes;
 - I. Identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from customer or through reliable and independent source.
 - II. Identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures to verify his identity so that the MFB is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement.

-
- III. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
 - IV. Monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the MFB's knowledge of the customers, their business and risk profile, including, where necessary, the source of funds and, updating records and data/ information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with MFB;
- j. **“Designated non-Financial Businesses and Professions (DNFBPs)”** means as defined under FATF Recommendations;
 - k. **“Domestic wire transfer”** means any wire transfer where the originator and beneficiary institutions are located in Pakistan regardless the system used to effect such wire transfer is located in another jurisdiction;
 - l. **“Dormant or in-Operative Account”** means the account in which no transaction has taken place during the preceding one year;
 - m. **“FATF Recommendations”** means the Recommendations of Financial Action Task Force as amended from time to time;
 - n. **“FMU”** means the Financial Monitoring Unit established under the AML Act 2010;
 - o. **“Electronic Fund transfer/wire transfer”** means any transaction carried out by financial institution on behalf of originator person by way of electronic means or otherwise to make an amount of money available to beneficiary person at another beneficiary institution, irrespective of whether the originator and the beneficiary are the same person;
 - p. **“Government entity”** means federal or provincial government, a ministry within such a government, a local government or an agency specially established by any such government, or a department, organization or corporation owned or controlled by such government under federal, provincial or local law;
 - q. **“Legal arrangements”** mean express trusts or other similar legal arrangements;
 - r. **“Legal persons”** mean entities (companies, bodies corporate, foundations etc.) other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property;
 - s. **“Intermediary institution”** is an intermediary in the wire transfer payment chain; that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution;
-

- t. **“Money Laundering and Financing of Terrorism or ML/TF”** has the same meaning as ascribed to them in AML Act 2010;
- u. **“Online transaction”** means deposit or withdrawal of cash using different branches of a MFB through electronic means;
- v. **“Ordering institution”** means the financial institution that initiates a wire transfer on the instructions of the wire transfer originator in transferring the funds;
- w. **“Originator”** means the person who allows or places the order to initiate a fund transfer/wire transfer or an online transaction;
- x. **“Person”** has the same meaning as ascribed to it under the AML Act 2010;
- y. **“Politically Exposed Persons or PEPs”** are individuals who are entrusted with prominent public functions either domestically or by a foreign country, or in an international organization, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations/departments/autonomous bodies. This does not intend to cover middle ranking or more junior individuals in the foregoing categories;
- z. **“Respondent bank”** means the bank or financial institution outside Pakistan to whom correspondent banking services in Pakistan are provided and vice versa;
- aa. **“Risk”** refers to risk associated with money laundering and financing of terrorism;
- bb. **“Senior management”** means the officer(s) not below the rank of Executive Vice President as designated by the board of a MFB for the purpose of AML/CFT regulations;
- cc. **“Suspicious Transaction Report or STR”** as ascribed in AML Act 2010; and
- dd. **“Walk-in-customer or Occasional Customer”** means the person conducting occasional transactions and is not a customer having relationship with the MFB.

MONEY LAUNDERING, TERRORIST FINANCING AND OTHER UNLAWFUL ACTIVITIES (M)

To safeguard Microfinance Banks (MFBs) from the threat of Money Laundering, Terrorist Financing and other related unlawful activities, the following minimum standards are required to be followed by all the MFBs. Microfinance banks are free to take additional measures as per risks involved in line with Financial Action Task Force (FATF) recommendations. MFBs shall ensure to develop and implement following policies within three months of issuance of these regulations.

Regulation M - 1: Customer Due Diligence (CDD)

- 1. Know Your Customer/ Customer Due Diligence Policy:** All MFBs shall formulate a comprehensive KYC/CDD policy duly approved by their Board of Directors. The policy shall be communicated down the line to relevant officers / staff. Copies of the KYC/CDD policy shall be submitted to the Agricultural Credit and Microfinance Department (AC&MFD) of the State Bank of Pakistan. Any change in policy shall also be conveyed to SBP within seven (07) days of its approval from the Board of Directors.

MFBs shall apply customer due diligence measures including identification and verification of customers before opening a new account or extending any credit facility or establishing new business relationships. MFBs shall take all reasonable measures to perform due diligence of their existing and prospective customers to establish their identity and to confirm that the customer is not exploiting microfinance banking channel for any criminal activity, money laundering or terrorist financing.

- 2. Identity of Individual Customers:** Identity of all the prospective customers shall be established with all reasonable efforts. Before establishing any banking relationship with the client, MFBs shall inter alia obtain, verify and record the following on KYC/CDD form or account opening form;
 - a) Full name as per identity document;
 - b) Computerized National Identity Card (CNIC)/Passport/National Identity Card for Overseas Pakistanis (NICOP)/Pakistan Origin Card (POC)/Alien Registration Card (ARC) number or where the customer is not a natural person, the registration/ incorporation number or business registration number (as applicable);
 - c) Existing residential address, registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable);
 - d) Date of birth, incorporation or registration (as applicable);
 - e) Nationality or place of birth, incorporation or registration (as applicable);
 - f) Nature of business, geographies involved and expected type of counter-parties (as applicable);
 - g) Purpose of account;
 - h) Type of account;
 - i) Source of earnings;

- j) Expected monthly credit turnover (amount and No. of transactions); and
- k) Normal or expected modes of transactions.

In case of a salaried person, MFBs shall obtain copy of his/her service card, or any other acceptable evidence of service in addition to the attested copy of CNIC/relevant identity document.

In case of an illiterate person, MFBs shall take additional measures such as recent photograph of the new account holder besides taking his/her right and left thumb impression on the specimen signature card.

In case of joint account, CDD measures on all the joint account holders shall be performed as if each of them were individual customers of the MFB.

MFBs may open account on the basis of attested copy of NADRA receipt/token for new CNIC, provided all other requirements of account opening under these regulations are complied with. MFBs shall, however, obtain copies of CNICs of such customers within three months of the opening of account to avoid penal action.

Moreover, MFBs shall scan all potential and existing customers to ensure that they are not on the list of proscribed/designated individuals/entities.

3. **Documents Required for Accounts:** For all accounts, list of the required documents is given in Annexure – H.
4. **Verification of the Identity:** MFB shall verify identities of the customers (natural persons) from NADRA and in case of legal persons, identities of their natural persons from relevant authorities or where necessary using other reliable, independent sources and retain on record copies of all reference documents used for identification and verification. Identity verification shall be the responsibility of concerned MFB for which the customer should neither be obligated nor the cost of such verification be passed on to the customers.
5. **Identification and Verification of Natural Persons Acting on Behalf of Customer:**

In cases where one or more natural persons are acting on behalf of a customer/ occasional customer/ walk-in customer or where customer is a legal person, MFB shall identify the natural person(s) who act on behalf of the customer and verify the identity of such persons. Authority of such persons to act on behalf of the customer shall be verified through documentary evidence, including specimen signature of the persons so authorized.
6. **Provisional Account Opening:** After establishing identity of the prospective customers MFBs are allowed to provisionally open accounts (restricting debits) during the verification process of CNIC, however customers must be appropriately informed about this. For the purpose, MFBs may accept initial deposit at the time of submission of necessary documents by their prospective customers (natural persons) subject to the following;
 - i. Completion of verification within five (05) working days from the date of

- application of account opening;
- ii. Initial deposit receipt will be issued with 'Disclaimer' that account shall be opened after completing necessary due diligence including NADRA verification through verisys or bio-metric technology;
- iii. A temporary account number shall be generated which will be validated after completion of due diligence process;
- iv. The Initial deposit (with no minimum balance restrictions) will be credited to customer's designated account only;
- v. No transaction in the account, issuance of cheque book/ATM card or any other instrument will be allowed until completion of verification of identity of the customer; However, in cases where customer's biometric impression is successfully verified from NADRA the MFB may instantly activate the account subject to satisfactory due diligence;
- vi. The MFBs will maintain a list of all such customers/accounts where the business relationship needed to be closed on account of negative verification;
- vii. MFBs shall guide the customers to visit relevant branch to get refund of initial deposit in case of negative NADRA verification; and
- viii. Management of related risks effectively during the period.

- 7. Micro-Saving Accounts:** These are privileged savings accounts offered only to low income and poor persons who are traditionally excluded from formal financial system. These accounts can be opened after establishing identity of customer only, and upon approval of the branch manager. Balance limits for such accounts shall, however, not exceed Rs. 100,000.

MFBs shall ensure proper systems and controls to avoid misuse of this relaxation. MFBs shall also conduct regular internal audit to review and assess effectiveness of the relevant controls. If there arise any doubt on the identity of the micro-saving account holder, MFB shall verify identity document of such account holders from NADRA and consider reporting of STR if circumstances so warrant.

MFBs shall also encourage women in remote areas to open accounts for saving and other purposes. If women in remote areas do not possess identity cards, MFB shall guide them for obtaining their own Computerized National identity Cards (CNIC). Meanwhile, MFBs may open their micro-saving accounts, on the basis of attested copy of CNIC of her father/husband, for six months only. MFBs shall also obtain any document related to account holder e.g., Nikah Nama, Birth Certificate, Driving License, Educational Degree/ Certificate, Pension Book or Insurance Certificate.

- 8. Identification and Verification of Beneficial Owner:** MFBs are required to identify and verify the customer and beneficial owner (natural person) in relation to a customer. If however, MFB is not satisfied considering relevant information or data obtained from reliable source it should not open the account or provide any service.

In cases where the customer is a legal person, MFBs are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- I. identity of the natural person(s) (if any) who ultimately has a controlling ownership;
- II. if there is doubt (under para I) as to whether the person(s) with the controlling ownership interest is the actual beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and
- III. if no natural person is identified (as referred in i and ii above), the identity of the relevant natural person who holds the position of senior managing official.

In case of legal arrangements, MFBs should identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- I. for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership); and
- II. for other types of legal arrangements, the identity of persons in equivalent or similar positions.

- 9. Dormant/In-Operative Accounts:** In case of dormant or in-operative accounts, MFBs may allow credit entries without changing at their own, the dormancy status of such accounts. Debit transactions/ withdrawals shall not be allowed until the account holder requests for activation and produces attested copy of his/her identity document, if already not available and MFB is satisfied with CDD of the customer.

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

- 10. Prohibition of personal accounts for business purposes:** MFBs shall not allow personal accounts to be used for business purposes except in cases of proprietorships, small businesses and professions where constituent documents are not available and the MFBs are satisfied with KYC profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status & nature of business of that customer.
- 11. Anonymous Accounts:** MFBs shall not allow opening and maintaining of anonymous or numbered accounts or accounts in the names of fictitious persons.
- 12. Purpose of Account / Relationship:** MFBs shall obtain from the customer intended purpose of account and likely sources of fund before starting any business relationship or opening of an account. Personal / individual accounts shall not be allowed to be used for charity purpose / collection of donation.

- 13. On-Going Customer Due Diligence:** Ongoing Customer Due Diligence is an essential aspect of

effective KYC/CDD procedures and applies to all customers to whom the MFB is offering any type of service(s). Ongoing due diligence includes monitoring and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, purpose of account, their business and risk profile, and where necessary, the source of funds. MFBs shall keep on conducting customer due diligence at reasonable periodic intervals or on significant occasions throughout the business relationship, e.g.;

- i. Nature of product and services requested by the customer changes;
- ii. Significant transaction or series of transactions take place; and
- iii. Significant change occurs in the way customer operates his account.

MFBs shall ensure that the copies of valid identity documents (like CNICs) along with other documents, data or information collected under CDD process is retained and kept up-to-date and relevant by undertaking reviews of existing records. Moreover, for customers that are legal persons or legal arrangements, MFBs shall take reasonable measures to understand the nature of customer's business and its ownership and control structure.

14. Enhanced Due Diligence (EDD): It is possible that certain customers/transactions may pose high risk to MFBs. The high risk factors must be defined in the KYC/CDD policy which may include the description of such customers, products, transaction channels and geographic elements. In particular, following shall also be considered for enhanced due diligence;

- i. Having suspicion of money laundering or terrorist financing;
- ii. Customers with links to offshore tax haven;
- iii. Customers are in cash based businesses and deal in high-value items and where customers have high net worth with no clearly identifiable source of income, etc.
- iv. MFBs have reason to believe that the customer has been refused banking facilities by another bank / DFI / MFB;
- v. The customer or beneficial owner is a PEP, or family member or close associate of a PEP;
- vi. While establishing business with Non-Governmental Organizations (NGOs) / Not-for-Profit Organizations (NPOs) and Charities;
- vii. Opening of correspondent banks' accounts, and taking appropriate measures to obtain all relevant information about the correspondent bank;
- viii. Customers from jurisdictions which have been identified for inadequate AML/CFT measures by FATF or called for by FATF for taking counter measures;
- ix. MFB has doubts about the veracity or adequacy of previously obtained identification data;
- x. Customer carries out occasional transactions that are wire transfers;
- xi. Dealing with Designated non-Financial Businesses and Professions (DNFBPs) especially in cases where underlying value of service exceeds a threshold approved by the board of directors; and
- xii. In case of PEPs and correspondent banking, MFBs are required to obtain senior management approval for establishing or continuing business relationship.

A. Dealing with foreign and domestic PEPs MFBs shall:

- a) put in place a risk management systems to determine whether a customer or the beneficial owner is a PEP, his/her family members or close associates;
- b) obtain senior management's approval before establishing (or continuing, for existing customers) such business relationships;
- c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- d) conduct enhanced ongoing monitoring on that relationship.

B. Dealing with NGOs/NPOs/ Charities' accounts

- a. MFBs should also conduct enhanced due diligence (including obtaining senior management approval) while establishing relationship with Non-Governmental Organizations (NGOs) / Not-for-Profit Organizations (NPOs) and Charities to ensure that these accounts are used for legitimate purposes and the transactions are commensurate with the stated objectives and purposes.
- b. These accounts should be opened in the name of relevant NGO/NPO/Charities as per title given in constituent documents of the entity. The individuals who are authorized to operate these accounts and members of their governing body should also be subject to comprehensive CDD. MFBs should ensure that these persons are not affiliated with any proscribed/ designated entity or person, whether under the same name or a different name.
- c. In case of advertisements through newspapers or any other medium, especially when bank account number is mentioned for donations, MFBs must ensure that the title of the account is the same as that of the entity soliciting donations. In case of any difference, immediate caution should be marked on such accounts and the matter should be considered for filing STR.
- d. Personal accounts shall not be allowed to be used for charity purposes/collection of donations.
- e. All existing relationships of NGOs/NPOs/Charities should be reviewed and monitored on an ongoing basis to ensure that these organizations, their authorized signatories, members of their governing body and the beneficial owners are not linked with any proscribed/ designated entity or person, whether under the same name or a different name. In case of any positive match, MFBs should consider filing STR and/or take other actions as per law.

The enhanced due diligence shall be in addition to CDD measures mentioned above in this framework.

15. Asset Side Customers: MFBs shall make comprehensive assessment of controls on asset products and related customers to ensure effective implementation of due diligence requirements as per

their own assessment of materiality and risk without compromising on identity and verification requirements. This shall include monitoring of the customers and related risks on ongoing basis as per standard norms and best practices to mitigate the risks related to such products/ customers.

16. Walk in Customer or Occasional Customer:

- i. MFBs shall obtain copy of CNIC (regardless of threshold) for online deposits/fund transfers and remittance through instruments such as DD, PO, MT etc. conducted by walk-in-customers;
- ii. MFBs shall obtain CNIC from walk-in customers conducting cash transactions above Rupees 0.5 million whether carried out in a single operation or in multiple operations that appears to be linked. If MFBs have a suspicion of money laundering or terrorist financing they must undertake appropriate CDD measures; and
- iii. For rest of transactions, identification requirements may be defined above an appropriate limit by MFBs themselves in their KYC/CDD policies.

17. Government Accounts: MFBs shall not allow opening of Government accounts in personal names of individuals. The Government account shall be opened on production of special resolution/authority from the concerned department duly endorsed by the Ministry of Finance (MoF) or Finance Department of the concerned (Provincial, Federal etc.) Government. This requirement is not applicable on institutions which do not fall under the purview of MoF. Further, Government accounts shall be operated by the designated officer(s) only.

18. Public Awareness Campaign on Requirement of CNIC: MFBs shall encourage customer services officers/tellers and other MFB staff, directly in touch with the customer, to create awareness on requirement of CNIC and shall facilitate/guide them to obtain CNIC.

19. New Technology: MFBs shall pay special attention to any threat that may arise from development of new products and new business practices, including new delivery mechanisms, and new or developing technologies, for both new and pre-existing products, that might favor anonymity and take measures, if required, to prevent their use in money laundering and/or terrorist financing schemes. Proper assessment of risks should be undertaken prior to the launch or use of such products, practices and technologies.

Measures for managing risks should include specific and effective CDD procedures that apply to non-face-to-face customers. In particular, MFBs should have policies and procedures in place to address anonymity risk associated with non-face-to-face customers / business relations/transactions. These policies and procedures should apply when establishing customer relationship and when conducting ongoing due diligence.

20. Non-Satisfactory KYC / CDD: In case, MFB is not able to satisfactorily complete the required CDD measures, account shall not be opened or any service provided and consideration should be given if the circumstances are suspicious so as to file an STR. If CDD of an existing customer is found unsatisfactory, the relationship should be treated as high risk and reporting of suspicious transaction be considered as per law and circumstances of the case.

21. Third party mandate: MFB shall verify that any person purporting to act on behalf of the actual customer is so authorized, and identify and verify the identity of that person. MFBs shall take reasonable measures, stipulated under para 8 above to identify the beneficial owner.

REGULATION M – 2: Wire Transfers/ Electronic Fund Transfers

The requirement under this Regulation shall apply to MFBs during the course of sending or receiving funds by wire transfer except transfer and settlement between the banks/MFBs where both the banks/MFBs are acting on their own behalf as originator and the beneficiary of the wire transfer. Moreover, while processing wire transfers, MFBs shall comply with relevant prohibitions on facilitating transactions, including freezing of funds/ accounts, of individuals and entities proscribed and/or designated under the Anti-Terrorism Act, 1997 and United Nations Security Council resolutions duly notified by the Ministry of Foreign Affairs.

1. Responsibility of the Ordering Institution

MFBs shall ensure that all wire transfers are accompanied by the following regardless of threshold:

- a. identify and verify the originator (if it has not already done under Regulation M1); and obtain details of beneficial owner(s) of funds; and
- b. record adequate details of the wire transfer so as to permit its reconstruction, including the date of the wire transfer, the type and amount of currency involved, the value date, the purpose and details of the wire transfer beneficiary and the beneficiary institution, and relationship between originator and beneficiary, as applicable etc.

MFB shall include the following information in the message or payment instruction, which should accompany or remain with the wire transfer throughout the payment chain:

- a. the name of the originator;
- b. the originator's account number (or unique reference number which permits traceability of the transaction);
- c. the originator's address or CNIC/passport number;
- d. the name of the beneficiary; and
- e. the beneficiary's address or CNIC/ passport number.

In cases where several individual wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information along with the beneficiary financial institution should be required to include the originator's account number or unique transaction reference number.

If the information accompanying the domestic wire transfer can be made available to the beneficiary financial institution and relevant authorities by other means, the ordering financial institution may only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering financial institution should be required to make the information available within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. The information should be available for immediate production to law enforcement

authorities, as per law.

The ordering financial institution shall not execute wire transfer if it does not comply with the requirements specified above.

2. Responsibility of the Beneficiary Institution

Beneficiary institution shall adopt risk-based internal policies, procedures and controls for identifying and handling incoming wire transfers that are not accompanied by complete originator and/ or beneficiary information. The incomplete originator and/or beneficiary information may be considered as a factor in assessing whether the transaction is suspicious and whether it merits reporting to FMU or termination thereof is necessary. MFBs shall remain cautious when entering into relationship or transactions with institutions which do not comply with the standard requirements set out for wire transfers by limiting or even terminating business relationship. In case of inward remittances, MFBs shall also receive a batch file, which contains details of several individual wire transfers from a single originator. However, in case of foreign inward remittances, local banks, that provide agency services to MFBs under agreement, shall be treated as originator and MFBs shall not take any foreign exchange exposure.

As beneficiary financial institutions, MFBs should take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify incoming cross-border wire transfers that lack required originator information or required beneficiary information. Moreover, MFBs should verify the identity of the beneficiary, if the identity has not been previously verified, and record this information.

3. Responsibility of Intermediary Institution

MFBs as an intermediary financial institution shall:

- (a) in passing onward the message or payment instruction, maintain all the required originator and beneficiary information with the wire transfer;
- (b) keep record of all the information received from the ordering financial institution or another intermediary financial institution, as per requirements of Regulation M-3: Record Retention;
- (c) take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or beneficiary information; and
- (d) have risk-based policies and procedures for determining:
 - i. when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information; and
 - ii. the appropriate follow-up action.

Regulation M - 3: Record Retention

The records of customer's CDD data and all transactions should be maintained by MFBs in systematic manner with exactness of period of preservation. For the purpose, following minimum requirements shall apply;

- i. **Identification Record:** MFBs shall keep record on the identification data obtained through the Customer Due Diligence (CDD) process, account files and business correspondence for at least Ten (10) years following the termination of the business relationship.
- ii. **Transactions Record:** MFBs shall maintain all necessary records on transactions, both domestic and international, for at least Ten (10) years following completion of the transaction. Such record must be sufficient for reconstruction of individual transactions so as to provide, if necessary, evidence for investigation or prosecution of criminal activity.

The examples of the necessary components of transaction record may include: customer's name (beneficiary's name), address, nature and date of transaction, type and amount of transaction, currency involved, type and identification of any account involved in the transaction.

MFBs must also maintain the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of ten years from completion of the transaction. The identification and transactions record besides results of analysis (if any) shall be made available to SBP or other domestic authorities that are competent, under law, to obtain this information and record.

MFBs shall, however, retain records for longer period where transactions and / or relationship relate to any investigation, litigation or required by the court of law or by any other competent authority.

Moreover, the transactions record may be maintained in paper or electronic form or on micro film, being sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity and admissible as evidence in a court of law.

Regulation M - 4: Reporting of Currency/Cash Transactions (CTR)

All MFBs shall adhere to the provision of Currency/Cash Transactions Report under the Anti-Money Laundering Act, 2010 and report currency/cash transactions to the Director General of the Financial Monitoring Unit (FMU). The Currency/Cash Transactions Guidance Notes and Reporting Form are available on the official website of FMU.

Regulation M - 5: Reporting of Suspicious Transactions (STR)

If an MFB suspects or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it shall report within seven days its suspicions to the Director General, Financial Monitoring Unit (FMU). The report should be on the format prescribed by FMU. Further, MFBs should file STR to report all attempted or conducted transactions, regardless of the amount of the transaction.

In instances where MFBs form a suspicion of money laundering or terrorist financing, and they reasonably

believe that performing the CDD process (as specified under M-1) will tip-off the customer, they are permitted not to pursue the CDD process, and instead file an STR.

The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.

MFBs shall intimate to State Bank of Pakistan on a bi-annual basis the number of STRs reported to FMU. The status reports indicating only the No. of STRs and not the contents of these STRs shall reach to Director, BPRD within seven days of close of each half year. MFBs, their Directors, Officers and Employees are strictly prohibited from disclosing (tipping-off) the fact that an STR or related information is being filled with the FMU. The red flag indicators are available in AML/CFT Regulations for Banks / DFIs at http://www.sbp.org.pk/l_frame/aml.htm

The employees of MFB are strictly prohibited to disclose the fact to the customer or any other quarter that a STR or related information is being or has been reported to any authority, except if required by law. This shall be made part of Code of ethics to be signed by employees and directors of the MFB.

Regulation M - 6: Implementation of obligations under United Nations Security Council (UNSC) Resolutions

MFBs shall ensure strict compliance of legal and regulatory requirements¹ including freezing actions and providing any banking services to proscribed²/designated³ individuals/ entities or their associated persons as per the Statutory Regulatory Orders (SROs)/Notifications issued by Federal Government from time to time under United Nations (Security Council) Act, 1948 to apply certain measures for giving effect to the decisions of the relevant United Nations Security Council resolutions, and, notifications issued under Anti Terrorism Act, 1997.

Before initiating banking relationships or allowing financial services, MFBs shall screen all customers to ensure they are not designated and/or proscribed. Further, in addition to measures prescribed under Regulation M-1 for Walk in customers MFBs may block all those identity documents, Passports and National Tax Numbers (NTNs) in their systems, which are on UNSC's list of proscribed /designated individuals/ entities and in SROs/Notifications in order to strengthen their controls against obtaining walk-in financial services by banned individuals.

Regulation M - 7: MFBs' Obligations

1. Internal AML/CFT policies, procedures & controls

Each MFB shall formulate risk based AML/CFT policy duly approved by their Board of Directors and cascade the same down the line to each and every business location and concerned employees for strict compliance. The detailed systems, procedures and controls shall also be developed by MFBs in the light of the policy approved by the board.

¹ Guidelines on Compliance of UNSC Resolutions revised from time to time.

² Proscribed under the Anti-Terrorism Act, 1997

³ Designated under the United Nations (Security Council) Act, 1948

The policies, procedures and controls shall include, amongst other things, CDD measures, record retention, correspondent banking, handling wire transfers, risk assessment procedures, the detection of unusual and/or suspicious transactions and the obligation to report suspicious transactions etc.

While formulating policies, procedures and controls, MFBs shall take into consideration money laundering and financing of terrorism threats that may arise from the use of new or developing technologies, agency agreements and outsourcing agreements especially those having features of anonymity or inconsistency with the spirit of CDD measures.

2. Utilization of Technology

MFBs shall utilize technological innovations to safeguard themselves from risks of Money Laundering/Terrorist Financing and other related risks. MFBs may therefore embed all KYC/CDD processes in their system and ensure installation of;

- a. Bio-metric machines at all branches for enabling usage of biometric technology for instant verification of particulars of prospective customers; and
- b. Transaction Monitoring Systems (TMS) that is capable of producing meaningful alerts based on pre-defined parameters/thresholds, for analysis and possible reporting of suspicious transactions. In this regard, they are required to implement appropriate TMS. The TMS may be customized in line with the size, nature and complexity of MFB's business environment and needs.

3. Compliance Function

MFBs shall have in place an appropriate setup to ensure AML/CFT compliance, including at least, the appointment of a 'Key Executive' officer as the compliance officer. A team of designated officers (regional/area/branch managers etc.) shall assist the compliance officer. Moreover, compliance and AML/CFT related responsibilities should be included as their Key Performance Indicators (KPIs). Further, ML/TF risks should also be included in KPIs of officer(s) responsible for Enterprise Risk Management and Operational Risk Management functions;

MFBs shall ensure that:

- a) Besides oversight by the Board, monitoring of compliance and AML/CFT function is assigned as term of reference to one of the Management Committees responsible for risk and control;
- b) The compliance officer, as well as persons appointed to assist him, have timely access to all customer records and other relevant information, which they may require to discharge their functions;
- c) Adequate staff is posted for carrying out CDD besides system based and/or otherwise monitoring and reporting of CTRs/STRs;
- d) Procedures are incorporated to record and maintain a database of:
 - I. account opening cases rejected by compliance or central account opening units,
 - II. the cases where customers' risk ratings recommended by business units were challenged or revised; and
 - III. the cases where accounts were closed based on ML/TF risks;
- e) Employees are not be assigned unrealistic business targets and conflicting roles;
- f) Appropriate strategies are devised to ensure provision of safe and smooth banking services; and

- g) Regular assessment is undertaken to evaluate:
 - I. Adequacy of compliance function's working strength; and
 - II. Deficiency if any, observed.

4. Internal Audit

MFBs shall maintain an independent internal audit function in line with Regulation G-6 "Internal Audit" and ensure that it remains adequately resourced and able to regularly assess the effectiveness of their internal policies, procedures and controls besides compliance with regulatory requirements and the underlying laws.

5. Employee Due Diligence

MFBs shall develop and implement a comprehensive employee due diligence policy and procedure to be implemented/ carried out at the time of hiring all employees; permanent, contractual, or through outsourcing. This shall include but not be limited to verification of antecedents and screening procedures to verify that person being inducted/hired has a clean history. Moreover, employees hired on a temporary/contractual basis, or through an outsourcing arrangement shall not be posted to work on critical areas, especially AML/CFT related functions.

6. Training

MFBs shall chalk out and implement suitable training programs for all relevant employees on an annual basis, in order to effectively implement the regulatory requirements besides MFBs' AML/ CFT related internal policies, procedures and controls. AML/CFT training combined with optimum use of technology is becoming inevitable due to ever changing nature of methods and trends in illicit activities, thus all relevant employees should be trained over the Transaction Monitoring System. It is also important to test the capability and knowledge of the relevant staff on periodic basis. For the purpose, MFB may either purchase or internally develop comprehensive AML/CFT Computer-based/Online Training Programs and Tests under a comprehensive plan with clear timelines for its implementation.

Annexure – H**DOCUMENTS TO BE OBTAINED FROM VARIOUS TYPES OF CUSTOMERS/ACCOUNT HOLDERS**

Sr. No.	Type of Customer	Documents/papers to be obtained
1	Individual	<p>A photocopy of any one of the following valid identity documents;</p> <ul style="list-style-type: none"> (I) Computerized National Identity Card (CNIC) issued by NADRA. (II) National Identity Card for Overseas Pakistani (NICOP) issued by NADRA. (III) Pakistan Origin Card (POC) issued by NADRA. (IV) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (V) Passport; having valid visa on it or any other proof of legal
2	Sole-proprietor	<ul style="list-style-type: none"> (i) Photocopy of identity document as per Sr. No. 1 above of the proprietor. (ii) Registration certificate for registered concerns. (iii) Sales tax registration or NTN, wherever applicable. (iv) Certificate or proof of membership of trade bodies etc, wherever applicable. (v) Declaration of sole proprietorship on business letterhead. (vi) Account opening requisition on business letter head
3	Partnership	<ul style="list-style-type: none"> (i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed' duly signed by all partners of the firm. (iii) Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. (iv) Authority letter from all partners, in original, authorizing the person(s) to operate firm's account.

4	Limited Companies/ Corporations	<ul style="list-style-type: none"> (i) Certified copies of: <ul style="list-style-type: none"> (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account (not applicable for Single Member Company); (b) Memorandum of Association; (c) Articles of Association (wherever applicable); (d) Certificate of Incorporation; (e) SECP registered declaration for commencement of business as required under Companies Act 2017; and (f) List(s) of Directors required to be filed under Companies Act 2017, as applicable. (ii) Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account; (iii) For individual (natural person) shareholders holding 20% or above stake (10% or above in case of EDD) in an entity, identification and verification of such natural persons; and (iv) For legal persons holding shares equal to 20% or above in an entity, identification and verification of individual (natural person) shareholders holding shares equal to 20% or above of that legal person.
5	Agents Accounts	<ul style="list-style-type: none"> (i) Certified copy of 'Power of Attorney' or 'Agency Agreement'. (ii) Photocopy of identity document as per Sr. No. 1 above of the agent and principal. (iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person.
6	Branch Office or Liaison Office of Foreign Companies	<ul style="list-style-type: none"> (i) A copy of permission letter from relevant authority i.e. Board of Investment. (ii) Photocopies of valid passports of all the signatories of account. (iii) List of directors on company letterhead or prescribed format under relevant laws/regulations. (iv) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account.

7	Trust, Clubs, Societies and Association etc.	<p>(i) Certified copies of: (a) Certificate of Registration/Instrument of Trust (b) By-laws/Rules & Regulations.</p> <p>(ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account.</p> <p>(iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.</p> <p>(iv) An undertaking signed by all the authorized persons on behalf of the institution mentioning that when any change takes place in the persons authorized to operate on the account, the banker will be informed immediately.</p>
8	Executors and Administrators	<p>(i) Attested copies of identity cards of the Executor / Administrator.</p> <p>(ii) Certified copy of Letter of Administration or Probate.</p>
9	NGOs/NPOs/ Charities	<p>(i) Certified copies of (a) Registration documents/certificate (b) By-laws/Rules & Regulations</p> <p>(ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account.</p> <p>(iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.</p> <p>(iv) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.</p>
10	Executors and Administrators	<p>(i) Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator.</p> <p>(ii) A certified copy of Letter of Administration or Probate.</p>
11	Minor Account	<p>(i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate) shall be obtained from minor.</p> <p>(ii) Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.</p>

Note:

- i. The photocopies of identity documents shall invariably be attested by Gazetted officer/ Nazim/Administrator or an officer of MFB after original seen.

-
- ii. In case of a salaried person, in addition to CNIC, an attested copy of his service card, or any other acceptable evidence of service, including, but not limited to a certificate from the employer will be obtained.
 - iii. In case of an individual with shaky/immature signatures, in addition to CNIC, a passport size photograph of the new account holder besides taking his right and left thumb impression on the specimen signature card will be obtained.
 - iv. In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that MFB shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account. For CNICs which expire during the course of the customer's banking relationship, MFBs shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, MFBs are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.
 - v. In case, the CNIC does not contain a photograph, MFBs shall obtain following:
 - a. A duly attested copy of either driving license, service card, Nikkah Nama, birth certificate, Educational degree/certificate, pension book, insurance certificate.
 - b. A photograph duly attested by gazetted officer/Nazim/Administrator/bank officer.
 - c. A copy of CNIC without photograph duly attested by the same person who attested the photograph.
 - vi. MFBs shall obtain copies of CNICs of all the members of Governing and Executive Bodies of DHA or ask for delegation of power to Administrator under section (7) & (8) of the Pakistan Defence Housing Authority Order, 1980 and accept copy of CNIC of Administrator as well as authorized signatories for the purpose of opening accounts of DHA or similar other authorities subject to compliance of other requirements.
 - vii. The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for opening bank accounts to the satisfaction of their banks.
 - viii. The requirement of obtaining NTN depends upon availability/issuance of NTN by tax authorities. The requirement of NTN should not be the reason for refusal of banking services to the customers, especially, where bank account is a prerequisite for obtaining NTN as per FBR's criteria. The MFBs should facilitate their customers in opening bank accounts and subsequently obtain NTN when issued by the FBR.
 - ix. The condition of obtaining photocopies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where MFBs

should obtain photocopies of identity documents of only those directors and persons who are authorized to open and operate the account. However, MFBs shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and 'Form 29' and verify their particulars through NADRA. The NADRA verification reports should be retained on record in lieu of photocopies of identity documents.
