INDEX

Guidelines on Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) Norms under Prevention of Money Laundering Act, PMLA, 2002 as amended by Prevention of Money Laundering (Amendment) Act, 2009 for International Money Transfer Services(Inward) under the Money Transfer Service Scheme (MTSS) and Money Changing Services in India Post

1. Introduction:

a. What is Money Laundering:

Money laundering may be defined as the process of changing large amounts of money that have been gained through illegitimate means to give it a legitimate appearance. Money evidently gained through crime is "dirty" money, and money that has been "laundered" to appear as if it came from a legitimate source is "clean" money. Money can be laundered by many methods, which vary in complexity and sophistication. Cash proceeds derived from illegal activity may be physically disposed or channeled through complex layers of financial transactions to disguise the audit trail and provide anonymity to the source of such funds. These layering processes could be integrated to provide legitimacy to the criminally derived wealth. These integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert to criminal activity –

Placement - the physical disposal of cash proceeds derived from illegal activity.

Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

b. What is Financing of Terrorism:

Financing of terrorism generally refers to carrying out transactions involving funds that may or may not be owned by terrorist, or that have been, or are intended to be, used to assist the commission of terrorism.

The Anti-Money Laundering Act defines a “terrorism financing offence” as any offence under the Penal Code. Essentially, financing of terrorism includes:

- providing or collecting property for carrying out an act of terrorism;
- providing services for terrorism purposes;
- arranging for retention or control of terrorist property; or
- dealing with terrorist property.

2. The objective of AML / KYC / CFT norms.

The objective of prescribing KYC / AML / CFT guidelines is to prevent money laundering or terrorist financing activities by use of the systems of cross border inward money transfer into India from all over the world under MTSS or by use of the system of purchase and / or sale of foreign currency notes / Travellers' cheques by Post Offices, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable Post Offices to know/ understand their customers and their financial dealings better, which in turn help them manage their risks prudently.

3. Definition of Customer: Who is called a customer under KYC norms for MTSS and Money Exchange

For the purpose of KYC policy for MTSS and Money Exchange , a 'customer' is defined as:-

- An individual who visits the Post Office in order to undertake (occasionally or regularly) any inward remittance transactions i.e to receive money sent by the sender abroad, or for sale / purchase of foreign currency notes / Traveller's Cheques.
- An individual on whose behalf the transaction has been undertaken. (i.e. beneficial owner).
- an entity that has a business relationship with the Post Office;

4. Customer Due Diligence(CDD)

Conducting Customer Due Diligence (CDD) implies that each Post Office obtains satisfactory evidence and properly establishes in its records, the identity and legal existence of any person doing any kind of business (receiving international money remittance or foreign exchange) with it. Such evidence must be substantiated by reliable and independent source documents

4.1 General Guidelines on CDD.

- Every Post Office must conduct customer due diligence, when:
  - establishing any business relationship with any customer;
  - it has any suspicion of money laundering or financing of terrorism; or
  - it has any doubt about the veracity or adequacy of previously obtained information.
- The customer due diligence undertaken by the Post Office should at least comprise the following:
  - identify and verify the customer;
  - identify and verify beneficial ownership and control of such transaction;
  - obtain information on the purpose and intended nature of the business relationship/transaction; and

- conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant.

➢ Unwillingness of the customer to provide the information requested and to cooperate with the customer due diligence process may itself be a factor of suspicion.

➢ The Post Office should not commence business relation or perform any transaction, or in the case of existing business relation, it should terminate such business relation if the customer fails to comply with the customer due diligence requirements and lodge a suspicious transaction report.

➢ All Post Offices should keep in mind that information collected from the customer for the purpose of undertaking inward remittance transaction or for the money changing activities is to be treated as confidential and details thereof are not to be divulged for cross selling or any other purposes

5. KYC Policy.

5.1 Customer Acceptance Policy:

a. General

i. No remittance / Forex transaction can be undertaken in anonymous or fictitious name(s) / benami. Post Offices should not allow any transaction in any anonymous or fictitious name (s) or on behalf of other persons whose identity has not been disclosed or cannot be verified.

ii. International Money Transfer Service permits only inward **personal** remittances into India such as remittances towards family maintenance and remittances favouring foreign tourists visiting India. Therefore **remittances sent between non-related persons needs to be monitored closely** and due diligence should be exercised before accepting such a customer.

iii. No Commercial transactions or transactions for investment / loans / charity / donations are allowed under International Money Transfer Service. Donations/contributions to charitable institutions/trusts, trade related remittances, remittance towards purchase of property, investments or credit to NRE Accounts shall not be made through this arrangement.

iv. Transactions under International Money Transfer Service or money changing in the name of minors are not allowed.

v. Customers receiving unusually more transactions frequently also require close monitoring.

vi. Remittances sent to persons not have actually met, to pay for travel etc are not acceptable.

vii. One receiver is using different IDs for different transactions is not acceptable.

viii. Customer producing forged or false IDs cannot be accepted.

ix. Transaction wherein there is no financial rationale behind money being received by a person. Example-Students, Youngster who are financially dependent on their parents and the parents are residing in India but someone else is sending money to them are not

acceptable.

x. Transactions wherein Foreigner visiting India is receiving money from a country which is not their Home Country need intensive 'due diligence'.

xi. Transactions wherein the sender is a Foreign Name but the receiver is an Indian national needs to be properly monitored and extra Customer Due Diligence to be exercised.

xii. Transactions wherein there doesn't seem to be an apparent family relations between the sender and the receiver.

xiii. Transactions wherein a same person is receiving money from different senders needs to be properly monitored and extra Customer Due Diligence to be exercised .

xiv. Transactions wherein receivers are different but sender is same needs to be properly monitored and extra Customer Due Diligence to be exercised.

xv. Post Offices should not undertake any transaction where it is unable to apply appropriate Customer Due Diligence (CDD) measures i.e. where Post Office is unable to verify the identity and / or obtain documents required as per the risk categorization due to non — cooperation of the customer or non- reliability of the data/information furnished to the Post Office. It is however, necessary to ensure that harassment of customers is also avoided. In the circumstances where the Post Office believes that it would no longer be satisfied that it knows true identity of the customer, Post Office shall file Suspicious Transaction Report (STR) with Financial Intelligence Unit-India (FIU-IND).

xvi. A profile (a separate sheet in a register) for each new customer should be prepared and maintained by the Post Office, based on risk categorization, containing information like nature of ID proof, number, date and office of issue of the ID proof , social and financial status. Due diligence will depend upon risk perceived by the Post office and the profile will be confidential document and details should not be divulged for cross selling or any other purposes.

xvii. The Post Master should periodically update customer identification data if there is any continuing relationship.

xviii. Whenever there is suspicion of Money Laundering or Terrorist Financing or other factors that give rise to a belief that customer poses a risk of money laundering or terrorist financing, Post Master should carry out full scale customer due diligence before making payment of remittance.

b. Risk perception: Categorization of customers based on risk perception

Level I.

- All international remittances upto Rs 50,000/-.
- Purchase of foreign currency notes and/ or Travellers' Cheques from customers for any amount less than Rs.50,000/- or its equivalent.

Level II.

- All international remittances above Rs 50,000/- upto Rs 1,00,000/-.
- Purchase of foreign currency notes and/ or Travellers' Cheques from customers for any amount in excess of Rs.50,000/- or its equivalent

Level III.

- All international remittances for family maintenance above Rs 1,00,000/- which are sent by the member of the family who has gone abroad.
- International Remittances for foreign tourists visiting India.
- Customers collecting remittances from a different city than what's mentioned in the photo ID.
- Transactions wherein there doesn't seem to be an apparent family relations between the sender and the receiver.
- Transactions coming from high risk countries – Iran, Korea, Algeria, Ecuador, Ethiopia, Indonesia, Kenya, Myanmar, Pakistan, Sao Tomé and Principe, Tanzania, Turkey, Vietnam, Yemen (list updated regularly on FATF website must be referred to).
- Customers receiving unusually more transactions frequently.
- Transactions wherein the sender is a Foreign Name but the receiver is an Indian.
- Transactions wherein Foreigner visiting India is receiving money from a country which is not his Home Country.
- Transactions wherein a same person is receiving money from different senders.
- Transactions wherein receivers are different but sender is same.
- Non-resident customers.
- Customers from countries that do not or insufficiently apply the FATF standards (List of countries regularly updated on FATF website to be referred to).
- High net worth individuals;
- Politically exposed persons (PEPs);
- Non-face to face customers ;
- Those with dubious reputation as per public information available etc.
- Intentional breakup of money changing transactions to a series of transactions < Rs 50,000/-

c. Documentation requirement.

- For every transaction undertaken, the Identification proof and address proof is to be taken.
- Originals should be personally checked and photographs on the documents matched with the customer.
- Documents such as Identity card issued by Election Commission / Ration Card / Passport / Driving License / Aadhaar card etc. having photo identity and current address can be accepted as ID & Address proof as a single document.
- If the address on the document submitted for identity proof by the prospective customer is same as that declared by him/her, the document may be accepted as a valid proof of both identity and address. If the address indicated on the document submitted for identity proof differs from the current address declared by the customer, a separate proof of address

should be obtained.

- In case of foreign tourists, copies of passport containing identification particulars and address, may be accepted as documentary proof for both identification as well as address. Further, a copy of the visa of non-residents, duly stamped by Indian Immigration authorities may also be obtained and kept on record. However, where neither passports contain any address nor foreign tourists are able to produce any address proof, Post Offices may obtain and keep on record, a copy of passport and visa duly stamped by the Indian Immigration authorities and a declaration duly signed from foreign tourists regarding the permanent address.

- For high-risk (Level III) transactions, additional identification and address proof should be taken apart from the regular proof taken.

5.2 Customer Identification Procedure(CIP) : How to establish the identification of the accepted customer:

i. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Post Offices need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional. Being satisfied means that the Post Office must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to Post Offices and a burdensome regime for the customers. The Post Offices should obtain sufficient identification data to verify the identity of the customer and his address/location.

ii. Post Offices should introduce a system of periodical updation of customer identification data (including photographs), if there is a continuing relationship.

iii. An indicative list of the type of documents / information that may be relied upon for customer identification is given hereunder. It is clarified that permanent correct address, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the Post Office for verification of the address of the customer. When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, Post Offices should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be.

Features	Indicative list of acceptable documents
For verifying the name of the customer (individual) **(Originals should be personally checked and photographs on the documents matched with the customer)**	**Attested (self / Gazetted Officer) copy of any one of the following valid and current documents having photograph:-** (i) Passport (ii) PAN Card (iii) Voters identity Card (iv) Driving license issued by respective state Road Transport Authorities in India. (Learners License issued in India and licenses issued by foreign countries are not permitted) (v) Identity Card issued by Central/State Governments, Armed Forces/Paramilitary Services/Public Sector Undertakings to their employees. (Subject to satisfaction of Post Master). IDs issued to civilian residents by Army/police are not accepted. (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of Post Master. (vii) UIDAI (Aadhaar) Card (Letter of acknowledgement for having applied Aadhaar Card is not accepted).
For verifying the address of the customer (individual) **(Originals should be personally checked and photographs on the documents matched with the customer)**	**Attested (self /Gazetted Officer) copy of any one of the following valid and current documents:-** (i) Telephone Bill of not more than 3 months old (ii) Bank account statement (iii) Letter from a recognized public authority (iv) Electricity bill of not more than 3 months old (v) Ration Card (vi)Letter from employer(subject to satisfaction of Post Master)

iv. Some close relatives, e.g. wife, son, daughter and parents etc. who live with their husband, father/ mother and son/ daughter, as the case may be, may find it difficult to undertake transactions with the Post Office as the utility bills required for the address verification are not in their name. In such cases, the Post Master can obtain **an** identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (Prospective Customer) wanting to undertake a transaction is a relative and is staying with him/her. The Post Master can use any supplementary evidence such as a letter received through post for further verification of the address. It may however be kept in mind that the purpose of these instructions should only be to establish the identity of the customer and not to cause any undue hardship to individuals who are, otherwise, classified as low risk customers.

v. Relationship with a business entity like a company / firm / trusts and foundations should be established only after conducting due diligence by obtaining and verifying suitable documents. Copies of all documents called for verification should be kept on record. Post Offices should obtain information on the purpose and intended nature of the business relationship. Post Offices should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions inorder to ensure that they are consistent with their knowledge of the customer, its business and risk profile. Post Ofices should ensure that documents, data or information collected under the Customer Due Diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships. When a business relationship is already in existence and it is not possible to perform customer due diligence on the customer in respect of business relationship, Post Offices should terminate the business relationship and make a Suspicious Transaction Report to FIU-IND. In the circumstances when there is reason to believe that the true identity of the customer (individual / business entity) is not known, the Post Office should also file an STR with FIU-IND.

vi. Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, *e.g.,* Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, *etc.* Post Offices should gather sufficient information on any person/customer of this category intending to undertake a transaction and check all the information available on the person in the public domain. Post Offices should verify the identity of the person and seek information about the source /s of wealth and source /s of funds before accepting the PEP as a customer. The decision to undertake a transaction with a PEP should be taken at a senior level. Post Offices should also subject such transactions to enhanced monitoring on an ongoing basis. The above norms may also be applied to transactions with the family members or close relatives of PEPs. The above norms may also be applied to customers who become PEPs subsequent to establishment of the business relationship. These instructions are also applicable to transactions where a PEP is the ultimate beneficial owner. Further, in regard to transactions in case of PEPs, it is reiterated that Post Offices should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are family members or close relatives of PEPs and transactions of which a PEP is the ultimate beneficial owner.

5.3 Procedure under KYC for Undertaking business

5.3.1 Payment to beneficiaries under Money Transfer.

a) For payment to beneficiaries, the identification documents, as mentioned above, should be verified and a copy retained. The copy of identification documents obtained should contain current and legible photograph of beneficiaries. Further, in the event of a beneficiary being discovered to have received funds on the basis of a photo ID which did not support his/ her photograph, action would also be initiated against the Post Office. Thereafter, in addition to this, the identification requirements for cash payment to beneficiary shall also include biometric identification of the beneficiary. This stipulation will ultimately be linked to UID when it is fully implemented.

b) A cap of US $ 2500 has been placed on individual remittances under the scheme. Amounts up to `50,000 may be paid in cash. Any amount exceeding this limit shall be paid only by means of cheque/D.D. /P.O., *etc.*, or credited directly to the beneficiary's bank account. However, in exceptional circumstances, where the beneficiary is a foreign tourist, higher amounts may be disbursed in cash. Only 30 remittances can be received by a single individual during a calendar year.

5.3.2 Purchase of foreign exchange from customers

a) For purchase of foreign currency notes and/ or Travellers' Cheques from customers for any amount less than Rs.50,000/- or its equivalent, photocopies of the identification document need not be obtained. However, full details of the identification document should be maintained. If the Post Office has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50000/-, the Post Office should verify identity and address of the customer and also consider filing a suspicious transaction report to FIU-IND.

b) For purchase of foreign currency notes and/ or Travellers' Cheques from customers for any amount equal to or in excess of Rs.50,000/- or its equivalent, the identification documents, as mentioned in the list of acceptable documents above, should be verified and copies retained.

c) Payments made to customers for purchase of Foreign currency

i. Requests for payment in cash in Indian Rupees to resident customers towards purchase of foreign currency notes and/ or Travellers' Cheques from them may be acceded to the extent of only US $ 1000 or its equivalent per transaction.

ii. Requests for payment in cash by foreign visitors / Non-Resident Indians may be acceded to the extent of only US $ 3000 or its equivalent.

iii. All purchases within one month, i.e. within 30 days from the date of last transaction, may be treated as single transaction for the above purpose and also for reporting purposes.

iv. In all other cases, Post Offices should make payment by way of 'Account Payee' cheque / demand draft only.

d) Where the amount of forex tendered for encashment by a non-resident or a person returning from abroad exceeds the limits prescribed for Currency Declaration Form (CDF), the Post Office should invariably insist for production of declaration in CDF.

e) In case of any suspicion of money laundering or terrorist financing, irrespective of the amount involved, enhanced Customer Due Diligence (CDD) should be applied. Whenever there is a suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not in fact pose a low risk, Post Offices should carry out a full scale CDD before undertaking any transaction for the customer.

5.3.3 Sale of Foreign Exchange to Customers

a) **In all cases of sale of foreign exchange, irrespective of the amount involved**, for identification purpose the passport of the customer should be insisted upon and sale of foreign exchange should be made only on personal application and after verification of the identification document. A copy of the identification document should be retained by the Post Office.

b) Payment in excess of Rs.50,000/- towards sale of foreign exchange should be received only by crossed cheque drawn on the bank account of the applicant's firm/ company sponsoring the visit of the applicant / Banker's cheque / Pay Order / Demand Draft. Such payment can also be received through debit cards/ credit cards/ prepaid cards provided (a) KYC/ AML / CFT guidelines are complied with, (b) sale of foreign currency/ issue of Foreign Currency Travellers' cheques is within the limits (credit/ prepaid cards) prescribed by the bank, (c) the purchaser of foreign currency/ Foreign Currency Travellers' cheque and the credit/ debit/ prepaid card holder is one and the same person.

c) All purchases made by a person within one month i.e. within 30 days from the date of last transaction, may be treated as single transaction for the above purpose and also for reporting purposes. For sale of foreign exchange to a person within his/her eligibility through more than one drawal within 30 days or for a single journey/visit abroad, Post Offices may receive second and subsequent payments only by crossed cheque drawn on the bank account of the applicant's firm/company sponsoring the visit of the applicant/Bank's cheque / Pay Order / Demand Draft / debit cards / credit cards / prepaid cards, if the total rupee payment, including payments on earlier drawal(s), exceeds Rs. 50,000/- on the second or subsequent drawals.

d) Encashment Certificate, wherever required, should also be insisted upon.

5.4 Monitoring of transactions

Ongoing monitoring is an essential element of effective KYC procedures. Post Offices can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the transaction. Post Offices should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk transactions have to be subjected to intensified monitoring. Every Post Office should set key indicators for such transactions, taking note of the background of the customer, such

as the country of origin, sources of funds, the type of transactions involved and other risk factors.

Post Offices should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds

Post Offices should examine the background and purpose of transactions with persons from jurisdictions included in the Financial Action Task Force (FATF) Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined and written findings together with all the documents should be retained and made available to the Reserve Bank/ other relevant authorities, on request.

- Attempted transactions.

Where the Post Office is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Post Office should not undertake the transaction. Under these circumstances, the Post Office should make a suspicious transactions report to FIU-IND in relation to the customer, even if the transaction is not put through.

5.5 Risk Management.

I. All customers according to the amount involved at the time of undertaking transactions have been categorized in the perspective of risk involved, as mentioned at 5.1 (b) above. However the following general guidelines may be referred to.

- For high risk (Level III) transactions, additional Photo ID Proof, which SHOULD be a currently valid Passport or UID Card (not letter), issued by UIDAI, in addition to the KYC documents that are taken for other transactions should be taken.
- For high risk (Level III) transactions, additional Address Proof, like a copy of the latest landline / mobile phone bill / electricity bill, in addition to the KYC documents that are taken for all transactions.
- Payments for **doubtful transactions** (where documentary information is complete but the customer / transaction raises any suspicion or doubt) should be made by Account Payee cheques for transactions amounting to Rs 20,000/- or above.
- Original Photo ID and Address proof should be checked and compared to the copies given for all transactions.
- It should be ensured that signature on the ID Proof matches the signature on forms filled up by the customers.
- All documents accepted from the customer should be self-attested by the customer.
- The photos affixed on the ID proof given by the customer should be matched with the customer actually undertaking the transaction.
- Any questions put forth while ensuring the genuineness of the customer should be properly recorded on the documents so as to keep a proof and record the circumstances which made the transactions appear genuine, especially in cases where prima facie the transactions might have raised some suspicion.

6. Inspection / Audit of AML / KYC documents / procedures

All Circles should ensure that there is regular auditing of the Post Offices in respect to compliances for AML / KYC norms regularly to ensure strict adherence to the KYC policies and procedures. The Inspectorial staff is well-versed with the AML / KYC norms and procedures and that the transactions are regularly checked during the course of visits and inspections of all the Inspectorial staff, for AML / KYC compliance. On-hand training to the Post Office staff should also be given regularly by these visiting officers to ensure that the staff is well-versed with the subject. Checks of all cross border inward remittance transactions under MTSS and Forex transactions should be done to verify that they have been undertaken in compliance with the anti-money laundering guidelines and have been reported whenever required to the concerned authorities. Compliance on the lapses, if any, recorded by the concurrent auditors should be put up to the higher authorities immediately.

7 Introduction to new technologies.

Post Offices should pay special attention to any money laundering threats that may arise from new or developing technologies including transactions through internet that might favour anonymity and take measures, to prevent their use for money laundering purposes and financing of terrorism activities.

8 Combating financing of terrorism.

a) In terms of PML Rules, suspicious transaction should include *inter alia* transactions which give rise to a reasonable ground of suspicion that these may involve the proceeds of an offence regardless of the value involved. Post Offices should, therefore, develop suitable mechanism for enhanced monitoring of transactions suspected of having terrorist links and swift identification of the transactions and making suitable reports to the FIU-IND on priority.

b) Post Offices are advised to take into account risks arising from the deficiencies in AML/CFT regime of certain jurisdictions, *viz.*, Iran, Uzbekistan, Pakistan, Turkmenistan, Sao Tome and Principe, Democratic People's Republic of Korea (DPRK), Bolivia, Cuba, Ethiopia, Kenya, Myanmar, Sri Lanka, Syria, Turkey and Nigeria, as identified in FATF Statement (www.fatf-gafi.org) issued from time to time, while dealing with individuals from these jurisdictions. In addition to FATF Statements circulated by the Reserve Bank of India from time to time, Post Offices should also consider using publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. All Post Offices are accordingly advised to take into account risks arising from the deficiencies in AML/CFT regime of these countries, while entering into business relationships and transactions with persons (including legal persons and other financial institutions) from or in these countries/ jurisdictions and give special attention to these cases.

9 Maintenance of records of transactions.

All post offices shall maintain the record of all transactions of money remittance and Forex including the record of:-

(a) All **cash** transactions of the value of more than Rs.10 lakh.

(b) All series of cash transactions which are less than Rs.10 lakh but are integrally connected and are carried out within one month period and totally exceed Rs.10 lakh.

(c) Any transaction where cash is accepted and forged or counterfeit currency notes are used or where forgery of valuable security or documents has taken place.

(d) Any attempted transaction involving forged or counterfeit currency notes, forged

documents.

(e) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

10. Definition of suspicious transaction:-

Suspicious Transaction means a transaction defined in clause (v) below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith-

(I) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the schedule to the Act, regardless of the value involved: or

(ii) appears to be made in circumstances of unusual or unjustified complexity : or

(iii) appears to have no economic rationale or bonafide purpose; or

(iv) give rise to a reasonable ground of suspicion that involve financing of the activities relating to terrorism;

(v) 'Transaction' includes exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means.

11. **Information to be preserved**

Post Offices are required to maintain all necessary information in respect of transactions to permit reconstruction of individual transactions including the following information:

a. the nature of the transaction;

b. the amount of the transaction and the currency in which it was denominated;

c. the date on which the transaction was conducted; and

d. the parties to the transaction.

12. **Maintenance and Preservation of Records**

There should be proper maintenance and preservation of transaction information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, Post Offices should maintain for at least **ten years** from the date of transaction, all necessary records of transactions, both with residents and non-residents, which will permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

Post Offices should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passport, driving license, PAN card, voter identity card issued by the Election Commission, utility bills, etc.) obtained while undertaking the transaction, are properly preserved for at least **ten years** from the date of cessation of the business relationship. The identification records and transaction data should be made available to the competent authorities upon request.

As mentioned in the foregoing paras, Post Offices have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including

all documents/office records / memoranda pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under Prevention of Money Laundering Act, (PMLA), 2002, as amended by Prevention of Money Laundering (Amendment) Act, 2009 and Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, as amended from time to time.

13. Reporting of Transactions:

Following types of transactions are to be reported:—

(a) All cash transactions of value more than Rs.10 Lakh.

(b) All series of cash transactions which are less than Rs.10 lakh but are integrally connected and are carried out within one month period and totally exceed Rs.10 lakh.

(c) Any transaction where cash is accepted and forged or counterfeit currency notes are used or where forgery of valuable Security or documents has taken place.

(d) Any attempted transaction involving forged or counterfeit currency notes, forged security or document.

(e) All suspicious transactions, involving domestic as well as International Remittances etc. irrespective of the amount of transaction.

13.1. Reporting schedule

Following norms should be strictly followed in case of International money remittance falls under the different categories:-

Types of Transactions	Method of reporting of transactions.
Cash Transactions (CTR) (a) All cash transactions more than Rs 10 Lakh. (b) All series of cash transactions which are less than Rs.10 Lakh but are integrally connected and are carried out within one month period and totally exceed Rs.10 lakh.	1.In-charge of every departmental Post Office will be personally responsible for preparation of list of transactions mentioning nature of transaction, amount, name and Address, date of transaction, place of transaction, PAN No. (if given) of sender/ receiver. He/She will be responsible for sending this list to Head of the Division on monthly basis **by 3rd working** day of the subsequent month. 2.Headof the Division will be personally responsible for sending post office wise list of such transactions of his Division to Head of Circle **by** 5th **working day** of the subsequent month 3. Head of the Circle will be responsible For sending the consolidated post office-wise list of such transactions to DDG (PCO), PMLA in Directorate **by** 8th **working day** of the subsequent month. **In case no such report is received from field units by due date, a NIL report should be sent to DDG (PCO), PMLA by the circle in Directorate**

Suspicious Transaction (STR)	1.In-charge of every departmental post office will **be**
(c) Any transaction where cash is accepted and forged or counterfeit currency notes are used or where forgery of documents has taken place. (d) Any attempted transaction involving forged or counterfeit currency notes, forged document. (e)All suspicious transactions irrespective of the amount of transaction,	Personally responsible for preparation of list of transactions mentioning nature of transaction, amount, name and address, date of transaction, place of transaction, PAN No. (if given) of sender/receiver and nature/reason of suspicion in detail and will be responsible for sending this list to **Head of the Division (by name) on the very same day.** 2.Head of the Division will be personally responsible for sending post office wise list of such transactions of his division to Head of Circle (by name) **on the very same day of the receipt of STR from P O** 3.Head of the Circle will be responsible for sending the consolidated post office-wise list of such STRs to DDG (Public Compliance Officer), PMLA (by name) at Directorate by **on the very same day of receipt of STR from D.O.**

Note 1:- It is likely that in some cases transactions are abandoned / aborted by customers on being asked to give some details or to provide documents. All such attempted transactions should also be reported like STRs irrespective of the amount of the transaction and even if the transaction is not completed by the customer.

Note 2:- Details of the customers along with transaction details should be reported in suspicious transaction where any customer is found doing deliberate splitting of amount to avoid reporting of cash transactions.

14 Attestation of KYC Documents

(i) At the time of undertaking remittance transaction, it should be ensured that all KYC documents have been self-attested. In case of illiterate customers, the documents are to be attested by any of the Gazetted Officer or Sarpanch Gram Panchayat or any Postal Staff or Gramin Dak Sewak after comparing with original.

(ii) It is the duty of PM/SPM/Supervisor (APM/DPM) to see that all KYC documents are having attestation as per clause (i)

15. Comparison of Address

PM/SPM/Supervisor (APM/DPM) shall ensure that address mentioned in the Booking/Receiving form is the same as mentioned in the address proof document.

16. Comparison of name

PM/SPM/Supervisor (APM/DPM) shall ensure that name of the sender/receiver mentioned in the Booking/Receiving form or receive form is the same as mentioned in the Identity proof document.

17. Recording of receipt of KYC Documents

PM/SPM/Supervisor (APM/DPM) shall record in writing under dated signatures on Booking/Receiving form as "KYC Documents verified & attached".

18 Customer Education/Employees' Training

a) Customer Education

Implementation of KYC procedures requires Post Offices to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for Circles to prepare specific literature/ pamphlets, *etc.*, so as to educate the customer of the objectives of the KYC programme. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

b) Employees' Training

Circles must have an ongoing employee training programme so that the members of the staff are adequately trained to be aware of the policies and procedures relating to prevention of money laundering, provisions of the PMLA and the need to monitor all transactions to ensure that no suspicious activity is being undertaken under the guise of remittances. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently. The steps to be taken when the staff come across any suspicious transactions (such as asking questions about the source of funds, checking the identification documents carefully, reporting immediately to the Principal Officer, *etc*.) should be carefully formulated by the Circles and there should be an ongoing training programme for consistent implementation of the AML measures.

Post Offices should take steps to identify and assess their Money Laundering/Terrorist Funding risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels, in addition to what has been prescribed in the paragraphs above. Post Offices would be required to adopt enhanced measures for products, services and customers with a medium or high risk rating. Post Offices may design risk parameters according to their activities for risk based transaction monitoring, which will help them in their own risk assessment.

(iii) The above KYC/ AML/ CFT Guidelines would also be applicable mutatis mutandis to all Post Offices and it will be the sole responsibility of the Postmasters to ensure that their locations adhere to these guidelines.