FOR'XCHANGE
INDIA CEMENTS CAPITAL LIMITED

POLICIES AND PROCEDURES FOR
Money Changing Activities & Money Transfer Service Scheme

Under

Anti Money Laundering Guidelines (AML)
Know Your Customer Norms (KYC)
&
Combating Financial Terrorism (CFT) Regulations

(Strictly for Internal Use only)

Reserve Bank of India with a view to curb Money Laundering activities have brought in a series of guidelines.

In terms of Prevention of Money Laundering Act, (PMLA), 2002, as amended by Prevention of Money Laundering (Amendment) Act, 2009, all Authorized Persons, authorized under Section 10(1) of FEMA, 1999 have been brought under the purview of PMLA, 2002. Therefore, the existing Know Your Customer (KYC) norms/ Anti-Money Launderings (AML) standards/ Combating the Financing of Terrorism (CFT) for money changing activities have been revisited in the context of the Financial Action Task Force (FATF) Recommendations on Anti Money Laundering (AML) standards and on combating the Financing of Terrorism (CFT). Detailed instructions on Know Your Customer (KYC) norms/ Anti-Money Launderings (AML) standards/ Combating the Financing of Terrorism (CFT) for money changing activities have been revised.

Further,

Attention of Authorized persons is invited to the Anti-Money Laundering Guidelines governing money changing transactions, issued vide A.P. (DIR Series) Circular No. 18 [A.P. (FL Series) Circular No. 01] dated December 02, 2005, A.P. (DIR Series) Circular No. 39 [A.P. (FL Series) Circular No. 2] dated June 26, 2006, A.P. (DIR Series) Circular No. 14 [A.P. (FL Series) Circular No. 1] dated October 17, 2007 and A.P. (DIR Series) Circular No. 15 [A.P. (FL Series) Circular No. 2] dated November 19, 2009.

SUBSEQUENTLY

Master Directions. DBR.AML.BC.NO.81/14.01.2001/2015-2016 – DATED FEB 25, 2016. Updated from Time to Time.

Rbi vide their Circular A.P. (DIR Series) Circular No.17
{A.P. (FL/RL Series) Circular No. 4 dated November 27, 2009]
Had brought in a series of changes to address

Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) standards/Combating the Financing of Terrorism (CFT) / Obligation of Branches under Prevention of Money Laundering Act, (PMLA), 2002, as amended by Prevention of Money Laundering (Amendment) Act, 2009 for Money Changing activities.

Company Policy

India Cements Capital Limited the group of the flagship company “The India Cements Limited” believes in conducting its business practices and processes in ethical manner abiding to all the guidelines set by RBI guidelines by virtue of FEMA and AML act.

The company restrains from unethical practices and has put in place control systems which are technologically superior, audit systems which are widely accepted, and adequate staff training to ensure and prevent Money Laundering and also ensure total compliance to RBI set guidelines.

Further to the RBI Circular, the company has framed a Policy & procedures on KYC / AML / CFT and obtained the Board approval on 30th Approval 2009. (Copy enclosed)

1. Introduction

- The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

- Eg. Illegal arms sales, smuggling, and the activities of organised crime, including for example drug trafficking and prostitution rings, etc. ,

- When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Anti-Money Laundering (AML) measures should include

- Identification of Customer according to "Know Your Customer" norms,
- Recognition, handling and disclosure of suspicious transactions,
- Branchpointment of Money Laundering Reporting Officer (MLRO),
- Staff Training,
- Maintenance of records, Audit of transactions.

2. Definition of Money Laundering

The offence of Money Laundering has been defined in Section 3 of the Prevention of Money Laundering Act, 2002 (PMLA) as "whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering". Money Laundering can be called a process by which money or other assets obtained as proceeds of crime are exchanged for "clean money" or other assets with no obvious link to their criminal origins.

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

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

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

III. 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 reenter the financial system appearing to be normal business funds.

If funds from criminal activity can be easily processed through a particular institution – either because its employees or directors have been bribed or because the institution turns a blind eye to the criminal nature of such funds – the institution could be drawn into active complicity with criminals and become part of the criminal network itself. Evidence of such complicity will have a damaging effect on the attitudes of other financial intermediaries and of regulatory authorities, as well as ordinary customers.

3 The objective

The objective of prescribing KYC/AML/CFT guidelines is to prevent the system of purchase and / or sale of foreign currency notes / Travelers' Cheques by the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable Branches to know / understand their customers and their financial dealings better which in turn help them manage their risks prudently.

4 Definition of Customer

For the purpose of KYC policy, a 'Customer' is defined as:

- A person who undertakes occasional / regular transactions;
- An entity that has a business relationship with the BRANCH;
- One on whose behalf the transaction is made (i.e. the beneficial owner).

5. Guidelines

5.1 General

It should keep in mind that the information collected from the customer while undertaking transactions is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Further, the team has to ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer, wherever necessary, should be sought separately with his/her consent.

5.2 KYC Policy

The Branch should frame their KYC policies incorporating the following four key elements:

a) Customer Acceptance Policy;
b) Customer Identification Procedures;
c) Monitoring of Transactions; and
d) Risk Management.

5.3 Customer Acceptance Policy (BRANCH)

The following Customer Acceptance Policy indicating the criteria for acceptance of customers is given to ensure that all our branches are KYC compliant :

i) No transaction is conducted in anonymous or fictitious / benami name(s).

ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status, etc. to enable categorization of customers into low, medium and high risk.

iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, (PMLA), 2002, as amended by Prevention of Money Laundering (Amendment) Act, 2009, 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 well as instructions/guidelines issued by the Reserve Bank, from time to time.

iv) Not to undertake any transaction where the BRANCH is unable to apply appropriate customer due diligence measures i.e. BRANCH is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the data/information furnished to the BRANCHES It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer.

v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out, the beneficial owner should be identified and all reasonable steps should be taken to verify his identity.

6. Customer Categorization

The branches should prepare a profile for each customer, based on risk categorization. The customer profile may contain information relating to customer's identity, his sources of funds, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by the branches However, the branch should take care to seek only such information from the customer, which is relevant to the risk category. However the branch should bear in mind that the Customer acceptance policy and its implementation does not become too restrictive and should not result in denial of money changing services to the general public.

6.1 Risk categorization shall be on the following basis.

i) Low Risk - Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions by whom by and large conform to the known profile, may be categorised as low risk.

Category of customers in Low Risk

a) Salaried employees
b) Customer belonging to lower economic strata and whose income is low
c) Government Companies
d) Government owned companies.

ii) **Medium Risk** - Customers that are likely to pose a higher than average risk should be categorized as medium depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Category of customers in Low Risk

a) Persons in business activity, trading, manufacturing, service, etc,.
b) Foreign exchange requirements do not commensurate with the profile of the company.
c) Further huge and frequent requirements of foreign exchange and also requesting for maximum limit.

iii) High Risk - The branches may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

iv) Category of customers in High Risk were due diligence is required.

(a) Non-resident customers;
(b) Customers from countries that do not or insufficiently apply the FATF standards;
(c) High net worth individuals;
(d) trusts, charities, NGOs and organizations receiving donations;
(e) Companies having close family shareholding or beneficial ownership;
(f) Firms with ' sleeping partners';
(g) Politically exposed persons (PEPs);
(h) Non-face to face customers; and
(i) Those with dubious reputation as per public information available etc.

It is important to bear in mind that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of money changing services to general public.

6.2 Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. The Branch need to obtain sufficient information from the customer necessary to establish, to their satisfaction, the identity of each new customer, whether occasional or business relationship, and the purpose of the intended nature of relationship. Being satisfied means that the BRANCH 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 The Branch and a burdensome regime for the customers. Besides risk perception, the nature of

information/documents required would also depend on the type of customer (individual, corporate, etc.).

For customers that are natural persons, the Branch should obtain sufficient identification document/s to verify the identity of the customer and his address/location.

For customers that are legal persons or entities, the BRANCH should

(i) verify the legal status of the legal person / entity through proper and relevant documents;
(ii) (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person; and
(iii) (iii) Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

For Customers who are close relatives of an individual.

Some close relatives, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, may find it difficult to undertake transactions with The Branch as the utility bills required for address verification are not in their name. It is clarified, that in such cases, The Branch 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 Branch can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, The Branch should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

Continuous Updation of documents

The Branch should introduce a system of periodic Updation of customer identification data (including photograph) if there is a continuing business relationship.

Address Proof

In addition to the identity proof the branch has to collect one of the following documents for address proof, namely:

1) Ration Card copy (2) Telephone Bill (3) Bank Statement (4) Electricity Bill
5) Corporation tax / water Tax receipt etc,. 6) LIC premium receipt,
7) Gas connection Receipt, etc,.

Customer Identification procedure Features from branches to be verified and documents that may be obtained from customers as per Circular. No.17, issued by RBI on 27.11.2009

Customer Identification Procedure
Features to be verified and documents
that may be obtained from customers

Features	Documents
Transactions with individuals	
- Legal name and any other names used	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (subject to the Branches satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the branch
- Correct permanent address	(i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the branch) (any one of the documents, which provides customer information to the satisfaction of the branch will suffice).

Establishment of business relationship- corporates - Name of the corporate - Principal place of business - Mailing address of the corporate - Telephone/Fax Number	Certified copy each of the following documents. (i) Certificate of incorporation (ii) Memorandum & Articles of Association (iii) Resolution of the Board of Directors for undertaking forex transactions with the branch (iv) PAN Card (v) Telephone Bill
Establishment of business relationship- partnership firms -Legal name -Address -Names of all partners and their addresses -Telephone/ Fax numbers of the firm and partners	One certified copy each of the following: (i) Registration certificate, if registered (ii) Partnership deed (iii) Any officially valid document identifying the partners and the persons holding the Power of Attorney, their addresses and their signatures. (iv) Telephone bill in the name of firm/ partners.
Establishment of business relationship- trusts and foundations -Names of trustees, settlers, beneficiaries and signatories -Names and addresses of the founder, the managers/ directors and the beneficiaries -Telephone/ Fax numbers	One certified copy of each of the following : (i) Registration certificate, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ managers/ directors and their addresses (iv) Resolution of the managing body of the foundation/ association (v) Telephone bill

6.3 Purchase of foreign exchange from customers

a. For purchase of foreign currency notes and/ or Travellers' Cheques from customers for any amount less than US $ 200 or its equivalent, photocopies of the identification document need not be obtained. However, full details of the identification document should be maintained. (Nevertheless it is suggested that the branches should collect a copy of the identity and attaché it along with the Encashment Certificate.

b. For purchase of foreign currency notes and/ or Travellers' Cheques from customers for any amount in excess of US $ 200 or its equivalent, the identification documents, as mentioned at (F-Part-II) annexed to this Circular, should be verified and a copy retained.

c. (a) 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 Rs.50000 or its equivalent per transaction.

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

e. All purchases within one month may be treated as single transaction for the above purpose and also for reporting purposes. A month is treated as 30 continuous days and not a calendar month.

f. In all other cases, The Branch should make payment by way of 'Account Payee's cheque / demand draft only.

g. 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 BRANCH should invariably insist for production of the declaration in CDF.

h. In case of any suspicion of money laundering or terrorist financing, irrespective of the amount involved, enhanced Customer Due Diligence (CDD) should be applied by the branches

6.4 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 BRANCHES

b) A customer can avail US $ 3000 or its equivalent in the form of currency notes, and the balance can be purchased by way of travellers cheques or prepaid cards under the LRS scheme for both private and Business visits in a financial year up to US $ 2,50,000.

c) 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 branch applicant's firm / company sponsoring the visit of the branch applicant / Banker's cheque / Pay Order / Demand Draft. Such payment can also be received through debit cards / credit cards / prepaid cards provided

   I. KYC/ AML guidelines are complied with,

   II. sale of foreign currency / issue of Foreign Currency Travellers' cheques is within the limits (credit / prepaid cards) prescribed by the bank,

   III. the purchaser of foreign currency / Foreign Currency Travellers' Cheque and the credit / debit / prepaid card holder is one and the same person.

   IV. All purchases made by a person within one month may be treated as single transaction for the above purpose and also for reporting purposes. (a month for this purpose is to be treated as a 30 day period and not calendar month).

   V. In case of sale of Forex against reconversion of Indian Currency to a non resident and Foreign Visitors, Encashment Certificate, where ever required should also be insisted upon. All conversions must be endorsed on the backside of the original Encashment Certificate and copy to be retained. .

6.5 Establishment of business relationship

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, as mentioned above. Copies of all documents called for verification should be kept on record.

Branches should obtain information on the purpose and intended nature of the business relationship. The Branch 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 customer, its business and risk profile. Branches 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, The Branch should terminate the business relationship and report to the Principal Office.

6.6 Customer Identification Requirements – Indicative Guidelines

i) Transactions by Trust/Nominee or Fiduciary Customers

There exists the possibility that trust/nominee or fiduciary relationship can be used to circumvent the customer identification procedures. The Branch should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, The Branch should insist on receipt of satisfactory document of identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While undertaking a transaction for a trust, The Branch should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. In all cases beneficiaries should be identified with reference to necessary documents. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries.

ii) Transactions by companies and firms

The Branch need to be vigilant against business entities being used by individuals as a ‘front’ for undertaking transactions with the Branches. The Branch should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a company that is listed on a recognized stock exchange, it will not be necessary to identify all the shareholders.

iii) Transactions by Politically Exposed Persons (PEPs)

Politically exposed persons 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.

The Branch should gather sufficient information on any person/customer of this category intending to undertake a transaction or establish a business relationship and check all the information available on the person in the public domain. The Branch should verify the identity of the person and seek information about the source of wealth and source 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 which should be clearly spelt out in Customer Acceptance Policy. The Branch 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. Where a customer subsequently becomes a PEP after a business relationship has already been established, enhanced CDD should be performed on such customers and decision to continue business relationship with the PEP should be taken at the level of Principal Officer or at HO.

7 Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Branch can effectively control and reduce their risk. However, the extent of monitoring will depend on the risk sensitivity of the transaction. The Branch should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

Transactions which are not normal and beyond US $ 10000 requires the HO's approval.

We have put in place a periodic review 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.

7.1 Attempted transactions

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

8 Suspicious Transactions

The Branch must ensure that its staff is vigilant against money laundering transactions at all times. An important part of the AML measures is determining whether a transaction is suspicious or not. A transaction may be of suspicious nature irrespective of the amount involved.

Some possible suspicious activity indicators are given below:

- Customer is reluctant to provide details/documents on frivolous grounds.
- The transaction is undertaken by one or more intermediaries to protect the identity of the beneficiary or hide their involvement.
- Large cash transactions.
- Size and frequency of transactions is high considering the normal business of the customer.
- Change in the pattern of business transacted.

The above list is only indicative and not exhaustive.

9 Risk Management

The company has put in place a proper KYC compliance system, proper management oversight, systems and controls, segregation of duties, training and other related matters. Policies and procedures are put in place for easy branch implementation.

Adequate Instructions have been given to the concurrent auditor and statutory auditor regarding the compliance functions who have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The statutory audit team has been given the role of an independent evaluation of the Branches own policies and procedures, including legal and regulatory requirements. The concurrent auditors should check all transactions 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 Branches, if any, recorded by the concurrent auditors should be put up to the Board. A certificate from the Statutory Auditors on the compliance with KYC / AML / CFT guidelines should be obtained at the time of preparation of the Annual Report and kept on record.

10 Foreign Currency - New Technologies- Pre-paid Cards

The company is tied up with the leading Principals (namely Issuers of Prepaid Products). While issuing these pre-paid cards, it should be ensured that all the KYC / AML/ CFT Guidelines are fully complied with.

All branches should pay special attention to any money laundering threats that may arise from new or developing technologies, that might favour anonymity and take measures, to prevent their use for money laundering purposes.

11. Combating Financing of Terrorism – (CFT)

11.1 What is terrorism

Terrorism is the systematic use of terror, often violent, especially as a means of coercion. Common definitions of terrorism refer only to those violent acts which are intended to create fear (terror), are perpetrated for a religious, political or, ideological goal; and deliberately target or disregard the safety of civilians.

11.2 Combating Financial Terrorism

a) In terms of PML Rules, suspicious transaction should include, inter alia transactions which give rise to a reasonable ground of suspicion that it may involve the proceeds of an offence mentioned in the Schedule to the PMLA, regardless of the value involved. The Branch should, therefore, develop suitable mechanism through appropriate policy framework for enhanced monitoring of transactions suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Principal Officer on priority.

b) The Branch 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, as identified in FATF Statement (www.fatf-gafi.org), issued from time to time, while dealing with individuals or businesses from these jurisdications.

12. Principal Officer

The company has appointed a Principal Officer responsible for collating information from the branches, monitoring and reporting transactions as required under the AML guidelines.

12.1 The Principal Officer

shall have reasonable access to all the necessary information/ documents, which would help him in effective discharge of his responsibilities.

Liaise with the relevant agencies like Reserve Bank of India, Enforcement, Financial Intelligence Unit, to support Money Laundering activities and combating financial terrorism.

The responsibility of the MLRO may include :

- Putting in place necessary controls for detection of suspicious transactions.
- Receiving disclosures related to suspicious transactions from the staff or otherwise.
- Deciding whether a transaction should be reported to the appropriate authorities
- Training of staff and preparing detailed guidelines / handbook for detection of suspicious transactions.
- Preparing annual reports on the adequacy or otherwise of systems and procedures in place to prevent money laundering and submit it to the Top Management within 3 months of the end of the financial year.

13 Maintenance of records of transactions / Information to be preserved / Maintenance and preservation of records / Cash and Suspicious Transactions Reporting to Financial Intelligence Unit- India (FIU-IND)

Branches should retain all the basic documents viz, Cash memo and Encashment certificates with the relevant supporting documents as required under KYC norms. These documents are subject to verification by our auditors internally and externally ad also by the regulatory and enforcing body. As the server is at HO the records are readily available in soft format and the branches are advised to maintain the hard copy as mentioned in te memorandum of instructions to Authorised persons.

13.1 Maintenance of records of transactions

The Branch should introduce a system of maintaining proper record of transactions prescribed under Rule 3, as mentioned below:

i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
ii) All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month; and
iii) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

13.2 Information to be preserved

The Branch are required to maintain the following information in respect of transactions

a) the nature of the transactions;
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

13.3 Maintenance and Preservation of Record

a) The Branch are required to maintain the records containing information in respect of all transactions that are undertaken.

b) The Branch should take appropriate steps to evolve a system for proper maintenance and preservation of transaction information (both in soft format and hard copy format) in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

c) The Branch should maintain for at least Five years from the date of transaction between the BRANCH and the client, 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.

d) The Branch 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 and during the course of business relationship, are properly preserved for at least FIVE years from the date of cessation of the transaction / business relationship. The identification records and transaction data should be made available to the competent authorities upon request.

e) The Branch has 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 includes all documents/office records / memoranda pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer's level 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 FIVE years as is required under PMLA, 2002

13.4 Anti Money laundering guidelines does not stop with ICCFL

- Each and every team member of For'Xchange should be aware of AML and its implication
- Each new team member should be made aware of AML and its implication
- The Scope and Application of AML extends to its Franchisees.
- It's our duty to explain the implications of AML to our Franchisees**.**

13.5 Reporting to Financial Intelligence Unit – India

Information relating to cash and suspicious transactions should be filed by the Principal Officer by the due dates to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

The Director,
Financial Intelligence Unit-India (FIU-IND)
6th Floor, Hotel Samrat,
Chanakybranchuri, New Delhi-110021.
Website - http://fiuindia.gov.in/

There are four reporting formats, as detailed in (F-Part-III) annexed to this circular, viz.

i) Cash Transactions Report (CTR);
ii) Electronic File Structure-CTR;
iii) Suspicious Transactions Report (STR);
iv) Electronic File Structure-STR.

The company has put in place a process to prepare a profile for each customer based on risk categorization. Further, the need for periodical review of risk categorization has been emphasized. Further we have also put in place appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

14 Customer Education/Employees' Training/Employees' Hiring

14.1 Customer Education

Implementation of KYC procedures requires certain information from a customer which may be of personal nature This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Hence it is mandatory on the branch team to educate the need for KYC norms.

It is the duty of the branch to ensure that the customer is not harassed under the guise of collecting information under KYC and hence need to keep the relevant RBI circulars / guidelines etc,. Handy and also displayed in front office to ensure total compliance by the customer.

14.2 Employees' Training

The company has the practice of conducting Annual Review meeting to access the performance of all the branches during March every year and during that time it is mandatory to have a training session on AML which is being done for the past 5 years. Further the training is imparted by the branch heads to their respective team members on their return to the branch which is being followed meticulously every year.

The training includes:

a) About the policies and procedures relating to prevention of money laundering, provisions of the PMLA
b) A Process has been put in place to monitor all transactions to ensure that no suspicious activity is being undertaken under the guise of money changing.
c) Training requirements for both marketing and back office staff is being imparted.
d) Action 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.)

14.3 Hiring of Employees

Out HR takes precautionary measures to ensure criminals are not allowed to misuse the system and get into employment.
Necessary references checks are done before issuing appoint order.

15. Policy Guidelines for MTSS transactions on AML Guidelines / KYC Norms and CFT Regulations

15.1 Introduction

RBI vide AP (DIR Series) Circular No. 15 dated 19th November, 2009 had notified the amendments carried out to prevention of Money laundering Act, 2002 (PMLA) vide prevention of Money Laundering (Amendment) Act, 2009. The said amendment which came into effect from 01.06.2009 has brought all Authorized Persons within the definition of "Financial Institutions" whereby all entities providing money changing and money transfer business are now within the ambit of the provisions of PMLA, 2002.

Subsequently, in terms of sub-rules 7 (i) of Government of India Notification No G.S.R.816 (E) dated 12.11.2009,RBI had published detailed guidelines on KYC / AML / CFT vide its AP (DIR Series) Circular No.18 dated 27.11.2009 for money transfer business.

The Said circular also mandated all Money Transfer Main Agents to:

(a) Have a revised Policy Framework on KYC / AML / CFT
(b) Prepare Customer Acceptance Policy / Customer Identification Procedures
(c) Appoint Principal Officer in Place of MLRO
(d) Place above the Board of Directors compliances on lapses, if any, reported by the Concurrent Auditors.

The Guidelines were also made applicable to the sub-agents of the Indian Main Agents under MTSS with a stipulation that "it will be the sole responsibility of the Indian Agents to ensure that their sub-agents also adhere to the said guidelines"

15.2 The Objective

KYC/AML/CFT policy of our company aims to prevent the system of cross border inward money transfer into India from all over the word under MTSS being user, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

15.3 Customer Acceptance Policy (CAP) of the company

The Customer Acceptance Policy has been framed in such a way that it is non-discriminative and in keeping with the spirit behind the guidelines of RBI. Our policy will always be customer friendly and we will not look at each and every customer with suspicion; but will be alert to detect suspicious transactions.

We will not undertake transactions lacking complete remitter information. We will not be bound to undertake transactions, if we are unable to undertake customer due diligence or obtain documents as required as per the risk categorization due to the non co-operation of the customer or non-reliability of the data/information furnished by him / her.

Enhanced due diligence will be applied while dealing with the Politically Exposed Persons (PEP's) which will be decided at the Corporate Office and all such cases will be categorized as High risk transactions.

Customer Acceptance Policy will always be based on the following:

(a)The Company shall ensure that no remittance is received in anonymous or fictitious / benami names.

All transactions will be put through only against.

- Application form (Receive Form)
- Personal identification of each customer provided the application is accompanied by valid identification documents.

(b) Our Customers are of the types viz

- Long-term customers-those who have been receiving remittances regularly through us and/or dealing with us on regular basis for our various other products and with whom we have built up relationship over a period of time.
- Walk in customers – First time recipients of MTSS

15.4 Risk Categorization for MTSS Transactions

Based on the above, the risk category of our customers is as under.

S.No.	Nature of the Customer	Risk
1	The customers who have dealing with us regularly and with whom we have built up relationship over a period of time and whose sources of wealth can be easily identifies.	Low
2	First time receipients of MTSS – transaction value up to Rs.10000/-	Low
3	First time receipients of MTSS – transaction value from Rs.10000/- to Rs.25,000/-	Medium*
4	First time receipients of MTSS – transaction value above Rs.25000/-	High*
5	Politically Exposed Persons (PEPs)	High
6	Remittances from Countries who are not members of FATF	High
7	Transactions with receiver from countries who are not members of FATF	High
8	Transactions from countries termed as terrorist grids	High

Note:*Risk category is Low if mode of payment is by way of crossed A/c Payee cheque.

The above parameters are only indicative. The risk perception will vary from customer to customer and will among other things depend upon

(a) Nature of the business activity
(b) Location
(c) Frequency of transaction
(d) Volume of transactions
(e) Mode of payments.
(f) Social/financial standing etc.

In case of any clarifications regarding the guidelines kindly speak to the Principal Officer and get it clarified immediately.

RECAP

Customer Identification Procedure

Features to be verified and documents that may be obtained from customers

Transactions with individuals

Legal name and any other names used

(i) Passport
(ii) PAN card
(iii) Voter's Identity Card
(iv) Driving license (v) Identity card (subject to the Branches satisfaction)
(v) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the branches.

Correct permanent address

(i) Telephone bill
(ii) Bank account statement
(iii) Letter from any recognized public authority
(iv) Electricity bill
(v) Ration card
(vi) Letter from employer (subject to satisfaction of the Branch).

(Any one of the documents, which provides customer information to the satisfaction of the branch, will suffice).

Establishment of business relationship- corporate

- Name of the corporate
- Principal place of business
- Mailing address of the corporate
- Telephone/Fax Number

Certified copy of each of the following documents.

(i) Certificate of incorporation
(ii) Memorandum & Articles of Association
(iii) Resolution of the Board of Directors for undertaking forex transactions with the BRANCH
(iv) Power of attorney granted to its managers, officers or employees to conduct forex transactions on behalf of the corporate and their identification.
(vi) PAN Card
(vii) (vi) Telephone Bill

Establishment of business relationship- partnership firms

-Legal name
-Address
-Names of all partners and their addresses
-Telephone/ Fax numbers of the firm and partners

One certified copy each of the following:
(i) Registration certificate, if registered
(ii) Partnership deed
(iii) Power of Attorney granted to a partner or an employee of the firm to transact Business on its behalf
(iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney, their addresses and their signatures.
(v) Telephone bill in the name of firm / partners.

Establishment of business relationship- trusts and foundations

-Names of trustees, settlers, beneficiaries and signatories
-Names and addresses of the founder, the managers/ directors and the beneficiaries
-Telephone/ Fax numbers

One certified copy of each of the following:
(i) Registration certificate, if registered
(ii) Power of Attorney granted to transact business on its behalf
(iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ managers/ directors and their addresses
(iv) Resolution of the managing body of the foundation/ association
(v) Telephone bill

The above KYC/AML/CFT FRAME WORK has been made in accordance with the guidelines issued by Reserve Bank of India from time to time. The said policy is subject to changes following the respective circulars as would be issued from time to time by Reserve Bank of India in the subject matter.

Contents of KYC / AML / CFT Guidelines