উত্তরবঙ্গ ক্ষেত্রীয় গ্রামীণ ব্যাংক
উত্তরবंग क्षेत्रीय ग्रामीण बैंक
UTTARBANGA KSHETRIYA GRAMIN BANK
(A GOVT. ENTERPRISE)
HEAD OFFICE, SUNITY ROAD, COOCHBEHAR – 736 101(WEST BENGAL)

C/45/ 23 /2020-21/F-KYC

Date: 18.07.2020

All Branches & Offices

Reg: **Adoption of RBI Master Circular on Master Direction-Know Your Customer(KYC) norms/Anti Money laundering(AML) standards/Combating Financing of Terrorism(CFT)/obligation of Banks and financial institutions under PMLA,2002 updated on July 01,2015**

Ref: 1. **RBI/2015 – 16/42-DBR.AML.BC.No.15/14.01.001/2015-16 dated July01,2015,**
2. **RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 updated on April 01,2020.**

We are enclosing herewith the 'Know your Customer(KYC), Anti Money Laundering(AML), updated on April 01,2020 /Combating Financing of Terrorism(CFT)/Obligation of Banks and financial Institutions under PMLA, 2002 updated on July 01,2015 duly approved by Our Honourable Board in its 248th meeting held on 29.06.2020.

General Manager-Operation Department has been nominated as Principal Officer by Honourable Board Of Bank for KYC/AML/CFT matters.

You are advised to go through the enclosed policy circular carefully and implement the policy in day-to-day banking Operation in the Branches.

This policy supersedes all existing KYC/AML/CFT policy of Bank.

Ensure compliance.

[D K Singh]
General Manager

Enclose:
1. RBI Master policy on AML RBI/2015-16/42-DBR.AML.BC.No. 15/14/14.01.001/2015-16 dated 01.07.2015
2. RBI Master Direction on KYC no DBR.AML.BC.No.81/14.01.001/2015-16 updated on 01.04.2020.

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2015 – 16/42
DBR.AML.BC.No.15/14.01.001/2015-16 **July 1, 2015**
Ashadha 10, 1937(saka)

The Chairpersons/Chief Executive Officers
All Scheduled Commercial Banks/ Regional Rural Banks / All India Financial Institutions/ Local Area Banks/ All Primary (Urban) Co-operative Banks /State and Central Co-operative Banks

Dear Sir/Madam

Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating Financing of Terrorism (CFT)/Obligation of banks and financial institutions under PMLA, 2002

Please refer to our Master Circular DBOD.AML.BC.No.22/14.01.001/ 14 –15 dated July 01, 2014 consolidating the instructions/guidelines issued till June 30, 2014 on the captioned subject.

2. This Master Circular consolidates instructions on the above matters issued up to June 30, 2015.

Yours faithfully,

(Lily Vadera)
Chief General Manager

Index

Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating Financing of Terrorism (CFT)/Obligation of banks and financial institutions under Prevention of Money Laundering Act, (PMLA), 2002.

A. Purpose

Banks and financial institutions (FIs) have been advised to follow certain customer identification procedure for opening of accounts and monitor transactions of suspicious nature for the purpose of reporting the same to appropriate authority. These 'Know Your Customer' (KYC) guidelines have been revisited in the context of the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). Detailed guidelines based on the recommendations of FATF and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS), with suggestions wherever considered necessary, have been issued. Banks/FIs have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of their Boards.

A list of circulars issued from time to time in this regard which are consolidated in this Master Circular is given in Annex – III

B. Application

(i) The instructions, contained in the Master Circular, are applicable to All India Financial Institutions, all Scheduled Commercial Banks (including RRBs), Local Area Banks,/ All Primary (Urban) Co-operative Banks /State and Central Co-operative Banks.

(ii) These guidelines are issued under Section 35A of the Banking Regulation Act, 1949 and Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act.

1. Introduction

The objective of KYC/AML/CFT guidelines is to prevent banks/FIs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks/FIs to know/understand their customers and their financial dealings better and manage their risks prudently.

2. Definitions

2.1 Customer

For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

2.2 Designated Director

"Designated Director" means a person designated by the reporting entity (bank, financial institution, etc.) to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes:-

(i) the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,

(ii) the Managing Partner if the reporting entity is a partnership firm,

(iii) the Proprietor if the reporting entity is a proprietorship concern,

(iv) the Managing Trustee if the reporting entity is a trust,

(v) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity, if the reporting entity is an unincorporated association or a body of individuals, and

(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

Explanation. - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act

2.3 “Officially valid document” (OVD)

OVD means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number, or any other document as notified by the Central Government in consultation with the Regulator.

(i) Provided that where ‘simplified measures’ are applied for verifying the identity of the clients the following documents shall be deemed to be OVD:

a) identity card with applicant’s Photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
b) Letter issued by a gazetted officer, with a duly attested photograph of the person.

(ii) Provided further that where ‘simplified measures’ are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be OVDs :.

a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
b) Property or Municipal Tax receipt;
c) Bank account or Post Office savings bank account statement;
d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
e) Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and

f) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

2.4 Person

In terms of PML Act a 'person' includes:

(i) an individual,

(ii) a Hindu undivided family,

(iii) a company,

(iv) a firm,

(v) an association of persons or a body of individuals, whether incorporated or not,

(vi) every artificial juridical person, not falling within any one of the above persons (i to v), and

(vii) any agency, office or branch owned or controlled by any of the above persons (i to vi).

2.5 Transaction

"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

(i) opening of an account;

(ii) deposits, withdrawal, 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;

(iii) the use of a safety deposit box or any other form of safe deposit;

(iv) entering into any fiduciary relationship;

(v) any payment made or received in whole or in part of any contractual or other legal obligation; or

(vi) establishing or creating a legal person or legal arrangement.

3. KYC Policy

Banks/FIs should frame their KYC policies incorporating the following four key elements:

(i) Customer Acceptance Policy (CAP);

(ii) Customer Identification Procedures (CIP);

(iii) Monitoring of Transactions; and

(iv) Risk Management.

3.1. Customer Acceptance Policy (CAP)

Banks/FIs should develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to the bank/FIs and including the following aspects of customer relationship in the bank/FIs.

(i) No account is opened in anonymous or fictitious/benami name.

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

(iii) Documents and other information to be collected from different categories of customers depending on perceived risk and the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time.

(iv) Not to open an account where the bank/FI is unable to apply appropriate customer due diligence measures, i.e., the bank/FI is unable to verify the identity and /or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The bank/FI may also consider closing an existing account under similar circumstances.

(v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking.

(vi) The bank/FI should have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

It is important to bear in mind that the adoption of customer acceptance policy and its implementation should not be too restrictive and which result in denial of banking facility to members of the general public, especially those, who are financially or socially disadvantaged.

3.2. Customer Identification Procedure (CIP)

3.2.1 General

(a) Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs. Banks/FIs need to obtain sufficient information to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the banking relationship. The bank/FI 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 banks/FIs and a burdensome regime for the customers.

(b) Banks/FIs should have a policy approved by their Boards which should clearly spell out the Customer Identification Procedure to be carried out at different stages, i.e.,

(i) while establishing a banking relationship;

(ii) while carrying out a financial transaction;

(iii) when the bank/FI has a doubt about the authenticity or adequacy of the customer identification data it has obtained;

(iv) when banks sell third party products as agents;

(v) while selling banks' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000/-.

(vi) when carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.

(vii) when a bank/FI has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

(c) Banks/FIs may seek 'mandatory' information required for KYC purpose which the customer is obliged to give while opening an account or during periodic updation. Other 'optional' customer details/additional information, if required, may be obtained separately after the account is opened only with the explicit consent of the customer.

3.2.2 I. Customer Due Diligence requirements (CDD) while opening accounts

A. Accounts of individuals:

(i) For opening accounts of individuals, banks/FIs should obtain one certified copy of an 'officially valid document' (as mentioned at paragraph 2.3 above) containing details of identity and address, one recent photograph and such other documents pertaining to the nature of business and financial status of the customer as may be required by the bank/FI.

(ii) E-KYC service of Unique Identification Authority of India (UIDAI) should also be accepted as a valid process for KYC verification under the PML Rules. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is to be treated as an 'Officially Valid Document'. Under e-KYC, the UIDAI transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/business correspondents/business facilitators, which may be accepted as valid process for KYC verification. The individual user, however, has to authorize to UIDAI by explicit consent to release her/his identity/address through biometric authentication to the banks/business correspondents/business facilitator. If the prospective customer knows only his/her Aadhaar number, the bank has to print the prospective customer's

e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned above. If the prospective customer carries a copy of the e-Aadhaar downloaded from a place/source elsewhere, still the bank has to print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal or adopt e-KYC procedure as mentioned above or confirm the identity and address of the resident through the authentication service of UIDAI

(iii) Since introduction is not necessary for opening of accounts under PML Act and Rules or the Reserve Bank's extant instructions, banks/FIs should not insist on introduction for opening of bank accounts.

(iv) **Simplified Measures for Proof of Identity:**

If an individual customer does not have any of the OVDs (as mentioned at paragraph 2.3 (i) above) as proof of identity, then banks/FIs are allowed to adopt 'Simplified Measures' in respect of 'Low risk' customers, taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. Accordingly, in respect of low risk category customers, where simplified measures are applied, it would be sufficient to obtain a certified copy of any one of the documents referred to at proviso to paragraph 2.3 (i) above., which shall be deemed as an OVD for the purpose of proof of identity.

(v) **Simplified Measures for Proof of Address:**

The additional documents mentioned at 2.3(ii) above shall be deemed to be OVDs under 'simplified measure' for the 'low risk' customers for the limited purpose of proof of address where customers are unable to produce any OVD for the same.

(vi) **Small Accounts**

If an individual customer does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as detailed at paragraph 2.3 above), then 'Small Accounts' may be opened for such an individual. A 'Small Account' means a savings account in which:

- the aggregate of all credits in a financial year does not exceed rupees one lakh;

- the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand and
- the balance at any point of time does not exceed rupees fifty thousand.

A ‘small account’ maybe opened on the basis of a self-attested photograph and affixation of signature or thumb print.

Such accounts may be opened and operated subject to the following conditions:

a) the designated officer of the bank, while opening the small account, certifies under his signature that the person opening the account has affixed her/his signature or thumb print, as the case may be, in her/his presence;

b) a small account shall be opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account and that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place;

c) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;

d) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism activity or other high risk scenarios, the identity of the customer shall be established through the production of “officially valid documents” and

e) foreign remittance shall not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of “officially valid documents”.

(vii) A customer is required to submit only one OVD for both proof of identity and for proof of address as part of KYC procedure. If the OVD submitted for proof of

identity does not have the proof of address (for e.g., PAN Card), then the customer is required to submit another OVD for proof of address.

(viii) Similarly, a customer is required to submit only one OVD as proof of address (either current or permanent) for KYC purpose. In case the proof of address furnished by the customer is neither the local address nor the address where the customer is currently residing, the bank should take a declaration from the customer of her/his local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted by the customer for such address. This address, however, should be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of letter, cheque books, ATM cards; telephonic conversation; visits to the place; etc. In the event of any change in this address due to relocation or any other reason, customers should intimate the new address for correspondence to the bank within two weeks of such a change.

(ix) In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address is to be submitted to the bank/FI within a period of six months.

(x) In case of close relatives, e.g. husband, wife, son, daughter and parents, etc. who live with their wife, husband, father/mother, daughter and son, who do not have officially valid document for address verification, then, in such cases, banks/FIs should obtain OVD for proof of address and identity of the relative with whom the prospective customer is living together with a declaration from the relative that the said person (prospective customer) proposing to open an account is a relative and is staying with her/him.

(xi) Banks are not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the bank to another branch of the same bank. Banks are advised that KYC verification once done by one branch of the bank should be valid for transfer of the account within the bank if full KYC verification has been done for the concerned account and is not due for periodic updation. The customers should be allowed to transfer their accounts from one branch to another branch without restrictions, without insisting on fresh proof of address and/or identity and on the basis of a self-declaration from the

account holder about his/her current address. Further, if an existing KYC compliant customer of a bank desires to open another account in the same bank, there should be no need for submission of fresh proof of identity and/or address.

(xii) Where a customer categorised as low risk expresses inability to complete the documentation requirements on account of any reason that the bank considers to be genuine, and where it is essential not to interrupt the normal conduct of business, the bank may complete the verification of identity within a period of six months from the date of establishment of the relationship.

(xiii) For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, banks/FIs may rely on a third party subject to the conditions that-

1) the bank/FI immediately obtains necessary information of such client due diligence carried out by the third party;
2) the bank/FI takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
3) the bank/FI is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;
4) the third party is not based in a country or jurisdiction assessed as high risk and
5) the bank/FI is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

(xiv) **Accounts of non-face-to-face customers**

With the introduction of phone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific

and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

(xv) **Procedure to be followed in respect of foreign students**

Banks should follow the following procedure for foreign students studying in India:

1) Banks may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
2) Banks should obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.
3) During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.
4) The account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.
5) Students with Pakistani and Bangladesh nationality will need prior approval of the Reserve Bank for opening the account.

(xvi) **Accounts of Politically Exposed Persons (PEPs) resident outside India**

1) Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on such person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly spelt out in the bank's Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an on-going basis. The above norms should also be applied to the accounts of the family members or close relatives of PEPs.

2) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, banks should obtain senior management's approval to continue the business relationship and subject the account to the CDD measures as applicable to PEPs including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

3) Further, banks should have appropriate ongoing risk management systems for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

B. Accounts of persons other than individuals:

(i) **Where the customer is a company***,* one certified copy each of the following documents are required for customer identification:

(a) Certificate of incorporation;

(b) Memorandum and Articles of Association;

(c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf and

(d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.

Banks/FIs need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks/FIs. Banks/FIs 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 public company it will not be necessary to identify all the shareholders.

(ii) Where the customer is a **partnership firm**, one certified copy of the following documents is required for customer identification:

(a) registration certificate;

(b) partnership deed and

(c) an officially valid document in respect of the person holding an attorney to transact on its behalf.

(iii) Where the customer is a **trust**, one certified copy of the following documents is required for customer identification:

(a) registration certificate;

(b) trust deed and

(c) an officially valid document in respect of the person holding a power of attorney to transact on its behalf.

(iv) Where the customer is an **unincorporated association or a body of individuals**, one certified copy of the following documents is required for customer identification:

(a) resolution of the managing body of such association or body of individuals;

(b) power of attorney granted to transact on its behalf;

(c) an officially valid document in respect of the person holding an attorney to transact on its behalf and

(d) such information as may be required by the bank/FI to collectively establish the legal existence of such an association or body of individuals.

(v) **Proprietary concerns***:*

(1) For proprietary concerns, in addition to the OVD applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern are required to be submitted:

(a) Registration certificate

(b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

(c) Sales and income tax returns.

(d) CST/VAT certificate.

(e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

(f) Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

(g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.

(h) Utility bills such as electricity, water, and landline telephone bills.

(2) Though the default rule is that any two documents, mentioned above, should be provided as activity proof by a proprietary concern, in cases where the banks are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the banks, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

(vi)**Simplified KYC norms for Foreign Portfolio Investors (FPIs)**

In terms of Rule 9 (14)(i) of the PML Rules, simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines

and have undergone the required KYC due diligence/verification prescribed by SEBI through a Custodian/Intermediary regulated by SEBI. Such eligible/registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank (as detailed in Annex II of the circular DBOD.AML.BC.No.103/14.01.001/2013-14 dated April 3, 2014) would be required. Category I FPIs are, however, not required to submit the undertaking that "upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank". For this purpose, banks/FIs may rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9 (2) [(a) to (e)] of the PML Rules.

(vii) **When the client accounts are opened by professional intermediaries:** When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks, however, should not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the banks. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look into the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

A gist of documents that can be accepted as proof of identity and address for various categories is furnished in Annex I

C. Beneficial ownership

When a bank/FI identifies a customer for opening an account, it should identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his identity, as per guidelines provided below:

(a) Where the **client is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.

Explanation- For the purpose of this sub-clause-

1. *"Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.*
2. *"Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.*

(b) Where the **client is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

(c) Where the **client is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

(d) Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(e) Where the **client is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person

exercising ultimate effective control over the trust through a chain of control or ownership.

(f) Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, banks/FIs should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks/FIs should insist on satisfactory evidence of the 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. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

II. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards

Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent the same being used for money laundering purposes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. Banks are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. It is desirable that agents are also subjected to due diligence and KYC measures.

III. Periodic updation of KYC

A. **CDD requirements for periodic updation:** Banks/FIs should carry out periodical updation of KYC information of every customer, which should include the following:

(i) KYC exercise should be done at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers. Such KYC exercise may include all measures for confirming the identity and address and other particulars of the customer that the bank/FI may consider reasonable and necessary based on the risk profile of the customer, taking into account whether and when client due diligence measures were last undertaken and the adequacy of data obtained.

(ii) Banks/FIs need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised as 'low risk', in case there is no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Banks/FIs should not insist on physical presence of such low risk customer at the time of periodic updation. The time limits prescribed at (i) above would apply from the date of opening of the account/ last verification of KYC.

(iii) Fresh photographs to be obtained from minor customer on becoming major.

B. **Freezing and closure of accounts**

(i) In case of non-compliance of KYC requirements by the customers despite repeated reminders by banks/FIs, banks/FIs may impose 'partial freezing' on such KYC non-compliant accounts in a phased manner.

(ii) During the course of such partial freezing, the account holders can revive their accounts by submitting the KYC documents as per instructions in force.

(iii) While imposing 'partial freezing', banks/FIs have to ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirements to be followed by a reminder giving a further period of three months.

(iv) Thereafter, banks/FIs may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts.

(v) If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' banks/FIs should disallow all debits and credits from/to the accounts thereby, rendering them inoperative.

(vi) Further, it would always be open to the bank/FI to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken at a reasonably senior level.

In the circumstances when a bank/FI believes that it would no longer be satisfied about the true identity of the account holder, the bank/FI should file a Suspicious Transaction Report (STR) with Financial Intelligence Unit – India (FIU-IND) under Department of Revenue, Ministry of Finance, Government of India.

IV. Miscellaneous

A. At-par cheque facility availed by co-operative banks

Some commercial banks have arrangements with co-operative banks under which the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangement, banks should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, banks should retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.

In this regard, Urban Cooperative Banks (UCBs) are advised to utilize the 'at par' cheque facility only for the following purposes:

(i) For their own use.

(ii) For their account holders who are KYC complaint provided that all transactions of Rs.50,000/- or more should be strictly by debit to the customer's account.

(iii) For walk-in customers against cash for less than Rs.50,000/- per individual.

In order to utilise the 'at par' cheque facility in the above manner, UCBs should maintain the following:

(i) Records pertaining to issuance of 'at par' cheques covering inter alia applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque.

(ii) Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

UCBs should also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved.

B. Operation of Bank Accounts & Money Mules

"Money Mules" can be used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules". In order to minimise the operations of such mule accounts, banks should strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

C. Simplified norms for Self Help Groups (SHGs)

KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG and KYC verification of all the office bearers would suffice. As regards KYC verification at the time of credit linking of SHGs, no separate KYC verification of the members or office bearers is necessary

D. Walk-in Customer

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. If a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the bank should verify the identity and address of the customer and also consider filing a Suspicious Transactions Report (STR) to Financial Intelligence Unit – India (FIU-IND).

In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.

E. Issue of Demand Drafts, etc, for more than Rs.50,000/-

Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rs.50,000/- and above is effected by debit to the customer's account or against cheques and not against cash payment.

Banks should not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.

F. Unique Customer Identification Code

A Unique Customer Identification Code (UCIC) will help banks to identify the customers, avoid multiple identities, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. Banks have been advised to allot UCIC while entering into new relationships with individual customers as also the existing customers.

3.3. Monitoring of Transactions

3.3.1 Ongoing monitoring

Ongoing monitoring is an essential element of effective KYC/AML procedures. Banks/FIs should exercise ongoing due diligence with respect to every customer and

closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence may be based on the following principles:

(a) The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.

(b) Banks/FIs should pay particular attention to the following types of transactions:

(i) large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.

(ii) transactions which exceed the thresholds prescribed for specific categories of accounts.

(iii) transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.

(iv) high account turnover inconsistent with the size of the balance maintained.

(c) Banks/FIs should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of not less than once in six months.

(d) Banks should closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Banks should analyse data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the bank and in case they find such unusual operations in their accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.

3.4. Risk Management

3.4.1 Banks/FIs should exercise on going 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 about the clients, their business and risk profile and where necessary, the source of funds.

The Board of Directors should ensure that an effective AML/CFT programme is in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters. In addition, the following may also be ensured for effectively implementing the AML/CFT requirements.

(i) Using a risk-based approach to address management and mitigation of various AML/CFT risks.

(ii) Allocation of responsibility for effective implementation of policies and procedures.

(iii) Independent evaluation by the compliance functions of bank/FI's policies and procedures, including legal and regulatory requirements.

(iv) Concurrent/internal audit to verify the compliance with KYC/AML policies and procedures.

(v) Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals.

3.4.2 (a) Banks/FIs should prepare a profile for each new customer based on risk categorisation. The customer profile should contain information relating to customer's identity, social/financial status, nature of business activity, information about the clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank/FI.

(b) Banks/FIs should categorise their customers into low, medium and high risk category based on their assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The banks/FIs are advised to have clear Board approved policies for risk categorisation and ensure that the same are meticulously complied with to effectively help in combating money laundering activities. The nature and extent of due diligence, may be based on the following principles:

(i) Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, may be categorised as low risk. Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc. Further, Non-Profit Organisations (NPOs)/ Non-Government Organisations (NGOs) promoted by the United Nations or its agencies, and such international/ multilateral organizations of repute, may also be classified as low risk customers.

(ii) Customers who are likely to pose a higher than average risk should be categorised as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, may, if considered necessary, be categorised as high risk.

The above guidelines for risk categorisation are indicative and banks/FIs may use their own judgement in arriving at the categorisation for each account based on their own assessment and risk perception of the customers and not merely based on any group or class they belong to. Banks may use for guidance in their own risk assessment, the reports and guidance notes on KYC/AML issued by the Indian Banks Association.

4. Correspondent Banking and Shell Bank

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks may take the following precautions while entering into a correspondent banking relationship:

(a) Gather sufficient information to fully understand the nature of business of the bank including information on management, major business activities, level of

AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country.

(b) Such relationships may be established only with the approval of the Board, or by a Committee headed by the Chairman/CEO with clearly laid down parameters for approving such relationships, as approved by the Board. Proposals approved by the Committee should be put up to the Board at its next meeting for post facto approval.

(c) The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented.

(d) In case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them.

(e) The correspondent bank should ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

(f) Banks should be cautious while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

(g) Banks should ensure that their respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

(h) Banks should not enter into a correspondent relationship with a **"**shell bank**"** (i.e., a bank which is incorporated in a country where it has no physical presence and is not affiliated to any regulated financial group).

(i) The correspondent bank should not permit its accounts to be used by shell banks.

5. Wire Transfer

Banks/FIs use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as rapid and secure method for transferring value from one location to another.

(a) The salient features of a wire transfer transaction are as under:

(i) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary could be the same person.

(ii) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.

(iii) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

(iv) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

(b) Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating the same. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold

limits. Accordingly, banks/FIs must ensure that all wire transfers are accompanied by the following information:

1. Cross-border wire transfers

(i) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

(ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

(iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

2. Domestic wire transfers

(i) Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

(ii) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50,000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.

(iii) When a credit or debit card is used to effect money transfer, necessary information as at (i) above should be included in the message.

(c) Exemptions

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

(d) Role of Ordering, Intermediary and Beneficiary banks

(i) Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of five years.

(ii) Intermediary bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for five years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

(iii) Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

6. Maintenance of KYC documents and Preservation period

PML Act and Rules cast certain obligations on the banks/FIs in regard to maintenance, preservation and reporting of customer account information. Banks/FIs are, therefore, advised to go through the provisions of the PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of the Act and the Rules *ibid.*

6.1 Maintenance of records of transactions

Banks/FIs should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

(i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

(ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which are that have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

(iii) All transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency [Ref: Government of India Notification dated November 12, 2009- Rule 3,sub-rule (1) clause (BA) of PML Rules]

(iv) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and

(v) All suspicious transactions, whether or not in cash, made as mentioned in the Rules.

Banks/FIs are required to maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following information:

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

6.2 Preservation of Records

Banks/FIs should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities

(i) In terms of PML Amendment Act 2012, banks/FIs should maintain for at least five years from the date of transaction between the bank/FI and the client, all necessary records of transactions, both domestic or international, 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.

(ii) Banks/FIs should ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills, etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules *ibid***.** The identification of records and transaction data should be made available to the competent authorities upon request.

(iii) Banks/FIs may maintain records of the identity of their clients, and records in respect of transactions referred to in Rule 3 in hard or soft format.

(iv) As mentioned in paragraph 3.3.1(i) of this Master Circular, banks/FIs are required 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/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors to scrutinize the 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.

7. Combating Financing of Terrorism

The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC).

(a) **The "Al-Qaida Sanctions List",** includes names of individuals and entities associated with the Al-Qaida. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml.

(b) The **"1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at http://www.un.org/sc/committees/ 1988/list.shtml.

The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Banks/FIs are required to update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, discussed below. Banks/FIs should ensure that they do not have any account in the name of individuals/entities appearing in the above lists. Details of accounts resembling any of the individuals/entities in the list should be reported to FIU-IND.

7.1 Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

(a) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 (Annex II of this circular) detailing the

procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

(b) Banks/FIs are required to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex II of this Master Circular) and ensure meticulous compliance to the Order issued by the Government.

7.2 Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) Banks/FIs are required to take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, banks/FIs should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that banks/FIs should also give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

(b) Banks/FIs should examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in 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 documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

8. Reporting Requirements

a) Reporting to Financial Intelligence Unit - India

(i) In terms of the Rule 3 of the PML (Maintenance of Records) Rules, 2005, banks/FIs are required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organisations (NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered (erstwhile Section 25 of Companies Act, 1956) under Section 8 of the Companies Act, 2013), cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

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

(ii) FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website. Banks/FIs should carefully go through all the reporting formats prescribed by FIU-IND.

(iii) FIU-IND have placed on their website editable electronic utilities to file electronic Cash Transactions Report (CTR)/ Suspicious Transactions Report (STR) to enable banks/FIs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore,

advised that in cases of those banks/FIs, where all the branches are not fully computerized, the Principal Officer of the bank/FI should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in

(iv) In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Banks/FIs are advised to take note of the timeliness of the reporting requirements.

In terms of instructions contained in paragraph 3.4 (b) of this Master Circular, banks/FIs are required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 3.2.2. (III), the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that, as a part of their transaction monitoring mechanism, banks/FIs are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of the customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

b) Reports to be furnished to FIU-IND

1. Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks/FIs should scrupulously adhere to the following:

(i) The CTR for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis and banks/FIs should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

(ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer of the bank to FIU-IND in the specified format(Counterfeit Currency Report – CCR), by 15th day of the next month. These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

(iii) While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.

(iv) CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.

(v) A summary of cash transaction reports for the bank as a whole should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-IND. In case of CTRs compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre, banks may generate centralised CTRs in respect of the branches under core banking solution at one point for onward transmission to FIU-IND, provided the CTR is to be generated in the format prescribed by FIU-IND;

(vi) A copy of the monthly CTR submitted to FIU-India in respect of the branches should be available at the branches for production to auditors/inspectors, when asked for; and

vii) The instruction on 'Maintenance of records of transactions'; and 'Preservation of records' as contained above in this Master Circular at Para 6.1 and 6.2 respectively should be scrupulously followed by the branches.

viii) However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.

2. Suspicious Transaction Reports (STR)

(i) While determining suspicious transactions, banks/FIs should be guided by the definition of suspicious transaction as contained in PMLA Rules as amended from time to time.

(ii) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. It is clarified that banks/FIs should report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction.

(iii) Banks/FIs should make STRs if they have reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

(iv) The STR should be furnished within seven days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

(v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in 'IBA's Guidance Note for Banks, January 2012'.

(vi) Banks/FIs should not put any restrictions on operations in the accounts where an STR has been filed. Banks/FIs and their employees should keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

3. Non-Profit Organisation

The report of all transactions involving receipts by non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency should be

submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

4. Cross-border Wire Transfer

Cross-border Wire Transfer Report (CWTR) is required to be filed with FIU-IND by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

9. General Guidelines

(i) **Confidentiality of customer information:**

Information collected from customers for the purpose of opening of account is to be treated as confidential and details thereof should not be divulged for the purpose of cross selling, etc. Information sought from the customer should be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer should be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It should be indicated clearly to the customer that providing such information is optional.

(ii) **Avoiding hardship to customers:**

While issuing operational instructions to branches, banks/FIs should keep in mind the spirit of the instructions issued by the Reserve Bank so as to avoid undue hardships to individuals who are otherwise classified as low risk customers.

(iii) **Sensitising customers:**

Implementation of AML/CFT policy may require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and may often lead to avoidable complaints and litigation. Banks/FIs should, therefore, prepare specific literature/pamphlets, etc., to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited.

(iv) **Hiring of Employees**

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking

channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks/FIs as an integral part of their personnel recruitment/hiring process.

(v) **Employee training:**

Banks/FIs must have an ongoing employee training programme so that the members of staff are adequately trained in AML/CFT policy. The focus of the training should be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff needs to be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues should be ensured.

(vi) **Provisions of FCRA**

Banks should ensure that the provisions of the Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

(vii) **Applicability to overseas branches/subsidiaries**

The guidelines in this circular apply to the branches and majority owned subsidiaries located abroad, to the extent local laws in the host country permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of the Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

(viii) **Technology requirements:**

The AML software in use at banks/FIs needs to be comprehensive and robust enough to capture all cash and other transactions, including those relating to walk-in customers, sale of gold/silver/platinum, payment of dues of credit cards/reloading of prepaid/travel cards, third party products, and transactions involving internal accounts of the bank.

(ix) **Designated Director***:*

Banks/FIs may nominate a Director on their Boards as “designated Director”, as required under provisions of the Prevention of Money Laundering (Maintenance

of Records) Rules, 2005 (Rules), to ensure compliance with the obligations under the Act and Rules. The name, designation and address of the Designated Director may be communicated to the FIU-IND. UCBs/ State Cooperative Banks / Central Cooperative Banks can also designate a person who holds the position of senior management or equivalent as a 'Designated Director'. However, in no case, the Principal Officer should be nominated as the 'Designated Director'.

(x) **Principal Officer:**

Banks/FIs may appoint a senior officer as Principal Officer (PO). The PO should be independent and report directly to the senior management or to the Board of Directors. The PO shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer may be communicated to the FIU-IND.

Annex- I

Customer Identification Procedure

Documents that may be obtained from customers

Customers/Clients	Documents (Certified copy of any one of the following officially valid document)
Accounts of individuals - Proof of Identity and Address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving License (v)Job Card issued by NREGA duly signed by an officer of the State Govt (vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number. Where 'simplified measures' are applied for verifying the identity of customers the following documents shall be deemed to be 'officially valid documents: i. identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; ii. letter issued by a gazetted officer, with a duly attested photograph of the person. Where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be OVDs :. i. Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);

	ii. Property or Municipal Tax receipt; iii. Bank account or Post Office savings bank account statement; iv. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; v. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and vi. Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.
Accounts of Companies	(a) Certificate of incorporation; (b) Memorandum and Articles of Association; (c) A resolution from the Board of Directors ar power of attorney granted to its manager officers or employees to transact on i behalf; and An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
Accounts of Partnership firms	(a) registration certificate; (b) partnership deed; and an officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Trusts	(a) registration certificate; (b) trust deed; and

	an officially valid document in respect of the person holding a power of attorney to transact on its behalf
Accounts of unincorporated association or a body of individuals	(a) resolution of the managing body of such association or body of individuals; (b) power of attorney granted to him to transact on its behalf; (c) an officially valid document in respect of the person holding an attorney to transact on its behalf; and (d) such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.
Accounts of Proprietorship Concerns Proof of the name, address and activity of the concern	Apart from Customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice • Registration certificate (in the case of a registered concern) • Certificate/licence issued by the Municipal authorities under Shop & Establishment Act, • Sales and income tax returns • CST/VAT certificate • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities • Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. The complete Income Tax return(not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities.

	In cases where the banks are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the banks, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

Annex II

File No.17015/10/2002-IS-VI
Government of India
Ministry of Home Affairs
Internal Security-I Division

New Delhi, dated 27th August, 2009

ORDER

Subject : Procedure for implementation of Section 51A of the Unlawful Activities (Prevention)Act, 1967

The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51A reads as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to –

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;

(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism",

The Unlawful Activities (Prevention) Act define "Order" as under:-

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

In order to expeditiously and effectively implement the provisions of Section 51A, the following procedures shall be followed:-

Appointment and Communication of details of UAPA nodal officers

2. As regards appointment and communication of details of UAPA nodal officers -

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), Ministry of Home Affairs. His contact details are 011-23092736(Tel), 011-23092569(Fax) and e-mail.

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA.

(iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA.

(iv) The IS-I Division in MHA would maintain the consolidated list of all UAPA nodal officers and forward the list to all other UAPA nodal officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA nodal officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA nodal officers should be circulated to the nodal officer of IS-I Division of MHA in July every year and on every change. Joint Secretary(IS-I), being the nodal officer of IS-I Division of MHA, shall cause the amended list of UAPA nodal officers to be circulated to the nodal officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, IS-I Division and Foreigners' Division in MHA.

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The IS-I Division of MHA would forward the designated lists to the UAPA nodal officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc.

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies requiring them to -

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(iii) The banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt**,** the banks stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts

covered by paragraph (ii) above , carried through or attempted, as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 3(ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the banks, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic assets or economic resources or related services available for the benefit of the designated individuals/entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act.

The order shall take place without prior notice to the designated individuals/entities.

Regarding financial assets or economic resources of the nature of immovable properties.

7. IS-I Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States and UTs with the request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction.

8. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA nodal officer of the State/UT would cause communication of the complete particulars of such individual/entity

along with complete details of the financial assets or economic resources of the nature of immovable property to the Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on **e-mail**

9. The UAPA nodal officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary(IS-I), Ministry of Home Affairs at the Fax telephone numbers and also on the e-mail id given below.

10. A copy of this reference should be sent to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail**.** MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT.

The order shall take place without prior notice, to the designated individuals/entities.

12. Further, the UAPA nodal officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the schedule to the order or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of the State/UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit,

terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

14. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

15. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in Regulators. FIU-IND and to the nodal officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

16. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of IS-I Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall take place without prior notice to the designated persons involved.

Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

17. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers.

18. The banks stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 4(ii) above within two working days.

19. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by IS-I Division of MHA.

Regarding prevention of entry into or transit through India

21. As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

Procedure for communication of compliance of action taken under Section 51A.

23. The nodal officers of IS-I Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the

individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

24. All concerned are requested to ensure strict compliance of this order.

(D .Diptivilasa)
Joint Secretary to Government of India

ANNEX –III

(List of Circulars on 'Know Your Customer' and monitoring of transactions consolidated in the Master Circular)

Sr. No.	Circular No. and date	Subject	Gist of instructions
1	DBOD.BP.BC.92/C.469-76 dated 12th August, 1976	Issue of DDs/TTs in excess of Rs.5,000/-	Applicants (whether customer or not) for DD/MT/TT/Travellers' cheques for amount exceeding Rs.10,000/- should affix Permanent Income Tax Number on the application.
2	DBOD.GC.BC.62/c.408(A)/87 dated 11th November, 1987	Frauds in banks-opening of new accounts.	Payment for imports should be made by debit to the accounts maintained with the same bank or any other bank and under no circumstances cash should be accepted for retirement of import bills. There should be reasonable gap of say, 6 months between the time an introducer opens his account and introduces another prospective account holder to the bank. Introduction of an account should enable proper identification of the person opening an account so that the person can be traced if the account is misused.
3	DBOD.BP.BC.114/C.469 (81)-91 dated 19th April, 1991	Misuse of banking channels for violation of fiscal laws and evasion of taxes – Issue and payment of demand drafts for Rs.50,000 and above.	Banks to issue traveilers' cheques, demand drafts, mail transfers, telegraphic transfers for Rs. 50,000/- and above by debit to customers' accounts or against cheques only and not against cash.
4	DBOD.BC.20/17.04.001/92 dated 25th August, 1992	Committee to enquire into various aspects relating to frauds and malpractices in	Banks advised to adhere to the prescribed norms and safeguards while opening accounts etc.

Sr. No.	Circular No. and date	Subject	Gist of instructions
		banks.	
5	DBOD.BP.BC.60/21.01.023/ 92 dated 21st December, 1992	Diversion of working capital funds.	Banks to ensure that withdrawals from cash credit/overdraft accounts are strictly for the purpose for which the credit limits were sanctioned by them. There should be no diversion of working capital finance for acquisition of fixed assets, investments in associate companies/ subsidiaries and acquisition of shares, debentures, units of UTI and other mutual funds and other investments in the capital market.
6	DBOD.FMC.No.153/27.01.0 03/93-94 dated 1st September, 1993	Monitoring of flow of funds.	Banks to be vigilant and ensure proper end use of bank funds/monitoring flow of funds. Banks to keep vigil over heavy cash withdrawals by account holders which may be disproportionate to their normal trade/business requirements and cases of unusual trends. Doubtful cases to be reported to DBOD, Regional office.
7	DBOD.GC.BC.193/17.04.00 1/93 dated 18th November, 1993	Frauds in banks – Encashment of Interest/Dividend Warrants, Refund Orders etc.	Banks to be vigilant in opening new accounts without proper introduction, new accounts with fictitious names and addresses. Banks instructed to strictly adhere to the instructions issued on opening and operating of bank accounts.
8	DBOD.GC.BC.202/17.04.00 1/93 dated 6th December, 1993	The Committee to enquire into various aspects relating to frauds and malpractices in banks.	Customer identification while opening accounts including obtaining of photographs of customers while opening accounts.
9	DBOD.No.GC.BC.46/17.04.0 01 dated 22nd April, 1994	The Committee to enquire into various aspects relating to frauds and	Clarifications given to banks regarding obtaining photographs of the depositors/account holder authorised to operate new

Sr. No.	Circular No. and date	Subject	Gist of instructions
		malpractices in banks.	accounts with effect from 1.1.1994. Obtaining of photographs would apply to residents and non-residents and all categories of deposits including fixed/recurring/cumulative deposit accounts and also to those persons authorised to operate the accounts.
10	DBOD.BP.BC.106/21.01.001 /94 dated 23rd September,1994	Fraudulent operations in deposit accounts-opening and collection of cheques/pay orders etc.	Banks to examine every request for opening joint accounts very carefully, look into the purpose, other relevant aspects relating to business, the financial position of the account holders and whether number of account holders are large. 'Generally crossed' cheques and payable to 'order' should be collected only on proper endorsement by the payee. Banks to exercise care in collection of cheques of large amounts and ensure that joint accounts are not used for benami transactions.
11	DBOD.BP.BC.57/21.01.001/ 95 dated 4th May, 1995	Frauds in banks – Monitoring of deposit accounts.	Banks to introduce system of close watch of new deposit accounts and monitoring of cash withdrawals and deposits for Rs.10 lakh and above in deposit, cash credit and overdraft accounts. Banks to keep record of details of these large cash transactions in a separate register.
12	DBOD.BP.BC.102/21.01.001 /95 dated 20th September, 1995	Monitoring of Deposit Accounts.	Reporting of all cash deposits and withdrawals of Rs.10 lakhs and above with full details in fortnightly statements by bank branches to their controlling offices. Transactions of suspicious nature to be apprised to Head Office.

Sr. No.	Circular No. and date	Subject	Gist of instructions
			RBI to look into these statements at the time of inspections
13	DBOD.BP.BC.42/21.01.001/ 96 dated 6th April, 1996	Monitoring cash deposits and withdrawals of Rs.10 lakh and above in deposit/other accounts.	Banks asked to submit feedback on implementation of the system of close monitoring of large cash deposits and withdrawals of Rs.10 lakh and above.
14	DBOD.No.BP.BC.12/21.01.023/98 dated 11th February 1998	Furnishing of data-violation of secrecy obligations.	Banks should satisfy themselves that information sought will not violate the laws relating to secrecy in banking transactions except under compulsion of law, duty to the public to disclose, where interest of bank requires disclosure and where disclosure is made with the express or implied consent of the customer.
15	DBS.FGV.BC.56.23.04.001/ 98-99 dated 21st June, 1999	Report of the Study Group on Large Value Bank Frauds.	Banks advised to implement the main recommendations of the Study Group on Large Value Bank Frauds.
16	DBOD.COMP.BC.No.130/07.03.23/2000-01 dated 14th June, 2001	Internet Banking in India-Guidelines.	Banking facilities on Internet will be subject to the existing regulatory framework. Banks having physical presence in India only will be allowed to offer banking services over Internet to residents in India and any cross border transactions will be subject to existing exchange control regulations. Banks to establish identity and also make enquiries about integrity and reputation of the prospective customer. Internet accounts should be opened only after proper introduction and physical verification of the identity of the customer.
17	DBOD.BP.52/21.01.001/2001-02 dated 5th December, 2001	Prevention of Terrorism Ordinance,2001-	Banks should keep a watchful eye on the transactions of the 23 terrorist organisations listed in the

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Implementation thereof.	Schedule to the Ordinance. Violations of the extant Acts or normal banking operations must be reported to the appropriate authorities under the Ordinance under advice to RBI. Banks to undertake 'due diligence' in respect of the 'KYC' principle.
18	DBOD.AML.BC.89/14.01.001/2001-02 dated 15th April, 2002	Freezing of funds pursuant to United Nations Security Council Resolution, 1390.	Accounts of individuals and entities listed should be immediately frozen as informed by the Security Council Sanctions Committee of the UN. If any transaction is detected involving any of these entities, banks to report to RBI promptly for necessary action.
19	DBOD.AML.BC.No.102/14.01.001/2001-02 dated 10th May, 2002	Monitoring of accounts - compliance with instructions.	Banks should ensure that no new accounts are opened by banned organisations. Banks to strictly adhere to the extant guidelines regarding opening and monitoring of accounts. Banks to confirm having issued instructions for immediate compliance by the branches and controlling offices.
20	DBOD.AML.BC.18/14.01.001/2002-03 dated August 16, 2002	Guidelines on "Know Your Customer" norms and "Cash transactions"	First circular on KYC. The customer identification should entail verification through an introductory reference from an existing account holder/a person known to the bank or on the basis of documents provided by the customer. The Board of Directors of the banks should have in place adequate policies that establish procedures to verify the *bona fide* identification of individual/ corporates opening an account. Branches of banks are required to report all cash deposits and withdrawals of Rs.10 lakhs and

Sr. No.	Circular No. and date	Subject	Gist of instructions
			above as well as transactions of suspicious nature with full details in fortnightly statements to their controlling offices.
21	DBOD.NO.AML.BC.58/14.01.001/2004-05 dated November 29, 2004	'Know Your Customer' (KYC)Guidelines – Anti Money Laundering Standards	Our guidelines were revisited to make those compliant with FATF recommendations and Basel Committee Report on CDD. Four pronged approach was prescribed to banks based on Customer Acceptance Policy, Customer Identification Procedure, Monitoring of Transaction and Risk Management.
22	DBOD.NO.AML.BC.28 /14.01.001/2005-06 dated August 23, 2005	Know YourCustomer Guidelines- Anti-Money Laundering Standards	KYC guidelines on document requirement were relaxed for people belonging to financially disadvantageous sections in the society, who could open account with introductory reference.
23	DBOD.NO.AML.BC.63/14.01.001/2005-06 dated February 15, 2006	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder	Reporting mechanism and formats were prescribed to banks to report cash and suspicious transactions to Financial Intelligence Unit- India (FIU-IND).
24	DBOD.AML.BC. No.77/ 14.01.001/2006-07 April 13, 2007	Wire transfers	Banks were advised to ensure that all wire transfers involving domestic and cross border fund transfers are accompanied by full originator information.
25	DBOD.AML.BC.No.63/ 14.01.001/2007-08 dated February 18, 2008	Know Your Customer (KYC) Norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)	Revised guidelines on KYC/AML issued on review of risk categorization of customers; periodical updation of customer identification data and screening mechanism for recruitment /hiring process of personnel.
26	DBOD.AML.BC.No.85/ 14.01.001/ 2007 -08 dated May 22, 2008	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules	Revised guidelines issued on CTR and STR by banks to FIU-IND.

Sr. No.	Circular No. and date	Subject	Gist of instructions
		notified thereunder.	
27	DBOD.AML.BC.No.12/14.01.001/2008-09 dated July 1, 2008	Master Circular – KYC norms/AML Standards/CFT/ Obligation of Banks under PMLA, 2002	The Master Circular consolidates all the guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30, 2008
28	DBOD.AML.BC.No.2/14.01.001/2009-10 dated July 1, 2009	Master Circular – KYC norms/AML Standards/CFT/ Obligation of Banks under PMLA, 2002	The Master Circular consolidates all the guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30, 2009
29	DBS.CO.FrMC.No.2605/23.04.001/2009-10 dated August 18, 2009	Adherence to KYC/AML Guidelines while opening & conducting accounts of MLM Companies	Banks were advised to exercise caution when opening accounts of marketing and trading firms and to monitor cases when large number of cheque books were issued to such companies and small deposits in cash were being made in a/cs.
30	DBOD.AML.BC.No.43/14.01.001/2009-10 dated September 11, 2009	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	The Government amended the Prevention of Money Laundering Act, 2005 and it came into force with effect from June 01, 2009 as notified by the Government.
31	DBOD.AML.BC.No.44/14.01.001/2009-10 dated September 17, 2009	Combating Financing of Terrorism-Unlawful Activities (Prevention) Act,(UAPA) 1967-Obligation of banks	Government of India, Ministry of Home Affairs issued an 'Order' dated August 27, 2009 detailing the procedure for implementation of Section 51A of UAPA
32	DBOD.AML.BC.No.68/14.01.001/2009-10 dated January 12, 2009	Prevention of Money laundering (Amendment) Rules 2009-Obligation of banks /Financial Institutions	Government of India Notification dated November 12, 2009 amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
33	DBOD.AML.BC.No.80/14.01.001/2009-10 dated March 26, 2010	Know Your Customer (KYC) guidelines-accounts of proprietary	Customer identification procedure issued for account opening by proprietary concerns.

Sr. No.	Circular No. and date	Subject	Gist of instructions
		concerns	
34	DBOD.AML.BC.No.95/14.01.001/2009-10 dated April 23, 2010	Prevention of Money Laundering (Maintenance of records of the …Intermediaries) Amendment Rules, 2010 - Obligation of banks	Government of India Notification dated February 12, 2010 amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
35	DBOD.AML.BC.No.108/14.01.001/2009-10 dated June 9, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Further clarifications issued to banks in regard to: suspicion of money laundering or terrorist financing; filing of STRs; PEPs and Principal Officer.
36	DBOD.AML.BC.No.109/14.01.001/2009-10 dated June 10, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Guidelines reiterated for Client accounts opened by professional intermediaries
37	DBOD.AML.BC.No.111/14.01.001/2009-10 dated June 15, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Banks advised to take into account risks arising from deficiencies in AML/CFT regime of the Jurisdictions included in FATF Statement and also publicly available information of countries which do not or insufficiently apply the FATF recommendations and banks should not enter into relationship with shell banks.
38	DBOD.AML.BC.No.113/14.01.001/2009-10 dated June 29, 2010	Prevention of Money Laundering (Maintenance of records of the …Intermediaries) Second Amendment Rules 2010	Government of India Notification dated June 16, 2010 amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
39	DBOD.AML.BC.No.38/14.01.001/2010-11 dated August 31, 2010	Accounts of proprietary concerns	An addition is made to the list of documents that may be accepted for opening a bank account in the name of a proprietary concern
40	DBOD.AML.BC.No.50/14.01.001/2010-11 dated October 26, 2010	Opening of bank accounts -salaried employees	Banks need to rely on certification only from corporates and other entities of repute and should be

Sr. No.	Circular No. and date	Subject	Gist of instructions
			aware of the competent authority designated by the concerned employer to issue such certificate/letter. In addition to the certificate from employer, banks should insist on at least one of the officially valid documents as provided in the PML Rules.
41	DBOD.AML.BC.No.65/14.01.001/2010-11 dated December 7, 2010	Operation of bank accounts & money mules	Banks advised that operations of money mules can be minimized if banks follow the guidelines contained in the Master Circular on KYC/AML/CFT/obligations of banks under PMLA, 2002
42	DBOD.AML.BC.No.70/14.01.001/2010-11 dated December 30, 2010	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as 'high risk'.	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'. requiring enhanced due diligence and intensified transaction monitoring. High risk associated with such accounts should also be taken into account to identify suspicious transactions for filing suspicious transaction reports (STRs) to FIU-IND.
43	DBOD.AML.BC.No.77/14.01.001/2010-11 dated January 27, 2011	Opening of "Small Account"	Government of India Notification dated December 16, 2011 amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005 to include definition of 'Small Account' and the detailed procedure for opening 'small accounts'.
44	DBOD.AML.BC. No.36/14.01.001/2011-12 dated September 28, 2011.	Know Your Customer Norms – Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and	Letter issued by the UIDAI is accepted as an officially valid document for opening all types of bank accounts

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Aadhaar number	
45	DBOD.AML BC.No.47/14.01.001/2011-12 dated November 04, 2011	Payment of Cheques/Drafts/ Pay Orders/Banker's Cheques	With effect from April 1, 2012, cheques / Drafts/ Pay Orders/ Banker's cheques issued on or after April 1, 2012 are valid for three months from the date of issue.
46	DBOD.AML.BC.No.65/14.01.001/2011-12 dated December 19, 2011	Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002-Assessment and Monitoring of Risk	Banks may take steps to identify and assess their ML/TF risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels. Banks should also have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk adopting a risk-based approach and adopt enhanced measures for products, services and customers with a medium or high risk rating.
47	DBOD AML BC No.70/14.01.001/2011-12 dated December 30, 2011	splitting of UNSC 1267 Committee's list of individuals and entities linked to Al-Qaida and Taliban	Banks may take into account both “Al-Qaida Sanctions List” and “1988 Sanctions List” for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.
48	DBOD.AML.BC. No 93 /14.01.001/2011-12 dated April 17, 2012	Know your Customer (KYC) guidelines - accounts of proprietary concerns	An addition is made to the list of documents that may be accepted for opening a bank account in the name of a sole proprietary concern
49	DBOD.AML.BC. No 109 /14.01.001/2011-12 dated June 08, 2012	Know your Customer (KYC) guidelines-Unique Customer Identification Code for bank customers in India	Banks to introduce Unique Customer Identification system to track all facilities availed, monitor transactions in a holistic manner and to have better risk-profiling of customers. System should be in place by May 2013.
50.	DBOD.AML.BC. No 110 /14.01.001/2011-12 dated June	Know your Customer (KYC)	Banks advised to complete the work of risk categorization and

Sr. No.	Circular No. and date	Subject	Gist of instructions
	08, 2012	guidelines - Risk Categorization and updation of Customer Profile	updation of risk profile of all customers by March 2013.
51	DBOD.AML.BC.No. 39/14.01.001/2012-13 dated September 7, 2012	Uploading of Reports in 'Test Mode' on FINnet Gateway	FIU-IND has advised that all banks should initiate submission of reports on the FINnet Gateway in TEST MODE from August 31, 2012 to test their ability to upload the report electronically.
52	DBOD.AML.BC. No. 49/14.01.001/2012-13 dated September 7, 2012	Uploading of Reports in 'Test Mode' on FINnet Gateway	FIU-IND has advised that all banks should 'go-live' from October 20, 2012 and banks may discontinue submission of reports in CD format and use only FINnet Gateway for uploading of reports in the new XML reporting format.
53	DBOD.AML.BC.No. 65/14.01.001/2012-13 dated December 10, 2012	Know Your Customer (KYC) norms /Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002	KYC norms were further simplified by issuing following instructions : (i) to have only one document for both identity and address if the address on the document submitted for identity proof is same as that declared in the account opening form, (ii) introduction from an existing customer of the bank not mandatory when documents of identity and address are provided, (iii) If the address provided by the account holder is the same as that on Aadhaar letter, it may be accepted as a proof of both identity and address, (iv) NREGA Job Card to be accepted as an 'officially valid document' for opening of bank accounts without the limitations applicable to 'Small Accounts'
54	DBOD.AML.BC. No.71/14.01.001/2012-13 dated January 18, 2013	Know Your Customer (KYC) Norms /Anti-Money Laundering (AML)	Procedure to identify beneficial owner as advised by Government has been specified.

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002	
55	DBOD.AML.BC. No. 78 /14.01.001/2012-13 dated January 29, 2013	Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002	To help a large number of customers with transferable jobs or those who migrate for jobs are unable to produce a utility bill or other documents in their name as address proof immediately after relocating, banks were advised to transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address, subject to submitting proof of address within a period of six months. Further, banks were also advised to accept rent agreement duly registered with State Government or similar registration authority indicating the address of the customer, in addition to other documents listed as proof of address in Annex I of our Master Circular on KYC/AML/CFT dated July 2, 2012.
56	RBI/2012-13/459DBOD.AML.BC.No.87/ 14.01.001/2012-13 dated March 28, 2013	Simplifying norms for Self Help Groups	KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG and KYC verification of all the office bearers would suffice. As regards KYC verification at the time of credit linking of SHGs, no

Sr. No.	Circular No. and date	Subject	Gist of instructions
			separate KYC verification of the members or office bearers is necessary
57	DBOD.AML.BC. No.101 /14.01.001/2011-12 dated May 31, 2013	Extending time period for allotting Unique Customer Identification Code (UCIC) for banks' customers in India	Considering the difficulties experienced in implementation the time for completing the process of allotting UCIC to existing customers was extended up to March 31, 2014.
58	DBOD.AML.BC.No.29 /14.01.001/2013-14 dated July 12, 2013	To reiterate and strengthen certain existing guidelines on KYC/AML/CFT for strict compliance.	Investigations by the Reserve Bank in the light of alleged violation of KYC/AML guidelines by several banks have shown that these guidelines have been violated, particularly in the case of walk-in customers. The circular was issued to reiterate and strengthen certain existing guidelines on KYC/AML/CFT for strict compliance.
59	DBOD.AML.BC.No.34/14.01. 001/2013-14 dated July 23, 2013	Simplifying norms for Periodical Updation of KYC	The issue was reviewed in the light of practical difficulties/constraints expressed by bankers/customers in obtaining/submitting fresh KYC documents at frequent intervals as the relative documents submitted earlier specially by low-risk customers have remained unchanged in most of the accounts. Accordingly, based on the suggestions received, revised instructions were received.
60	DBOD.AML.BC.No.44/14.01. 001/2013-14 dated September 2, 2013	e-KYC Service of UIDAI – Recognising on-line Aadhaar authentication (electronic verification process) to be accepted as an 'Officially Valid	In order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, e-KYC service UIDAI has launched its. Accordingly, it has been decided to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules,

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Document' under PML Rules	2005
61	DBOD.AML.BC.No.45/14.01.001/2013-14 dated September 2, 2013	Foreign students studying in India – KYC procedure for opening of bank accounts	Considering the difficulties faced by foreign students arriving in India in complying with the Know Your Customer (KYC) norms while opening a bank account due to non-availability of any proof of local address, norms were relaxed by allowing a time of one month for furnishing the proof of local address.
62	DBOD.AML.BC. No. 50/14.01.001/2013-14 dated September 3, 2013	Circular regarding Information sought by banks from customers	Banks were advised to collect only 'mandatory' information required for KYC purpose while opening an account and Other 'optional' customer details/additional information, if required may be obtained separately after the account is opened only with the explicit consent of the customer. Further, it was reiterated that banks should keep in mind that the information (both 'mandatory' – before opening the account as well as 'optional'- after opening the account with the explicit consent of the customer) collected from the customer is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes
63	DBOD.AML.BC.No.63/14.01.001/2013-14 October 29, 2013	Due diligence in correspondent banking relationship	Some commercial banks have arrangements with co-operative banks wherein the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for facilitating their remittances and payments. Since the 'at par'

Sr. No.	Circular No. and date	Subject	Gist of instructions
			facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangements, banks should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, banks should retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.
64	DBOD.AML.BC.No.80/14.01.001/2013-14 dated December 31, 2013	Amendment to Section 13(2) of PML Act	Banks have been advised to nominate a Director on their Boards as "designated Director" to ensure compliance with the obligations under Section 13(2) of the Prevention of Money Laundering (Amendment) Act, 2012.
65	DBOD.AML.BC.No.100/14.01.001/2013-14 dated March 4, 2014	Recognising E-Aadhaar as an 'Officially Valid Document' under PML Rules	Banks have been advised to accept e-Aadhaar downloaded from UIDAI website as an officially valid document subject to the following: a) If the prospective customer knows only his/her Aadhaar number, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the circular referred in paragraph 2 above. b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI

Sr. No.	Circular No. and date	Subject	Gist of instructions
			portal; or adopt e-KYC procedure as mentioned in the circular referred in paragraph 2 above; or confirm identity and address of the resident through simple authentication service of UIDAI.
66	DBOD.AML.No.16415/14.01.001/2013-14 dated March 28, 2014	Reporting of Cross Border Wire Transfer Report on FINnet Gateway	As per advice of FIU-IND a new reporting format for reporting of cross border wire transfers has been introduced. This was necessitated by amendments to Prevention of Money Laundering (PML) Rules, notified by the Government of India vide Notification No. 12 of 2013 dated August 27, 2013 and in terms of amended Rule 3, every reporting entity is required to maintain the record of all transactions including the record of all cross border wire transfers of more than Rs. 5 lakh or its equivalent in foreign currency, where either the origin or destination of the fund is in India.
67	DBOD.AML.BC.No.103/14.01.001/2013-14 dated April 3, 2014	Harmonization of KYC norms for Foreign Portfolio Investors (FPIs)	KYC norms in case of FPIs for opening bank accounts were rationalised of along the lines of instructions issued by SEBI.
68	DBOD.AML.BC.No.119/14.01.001/2013-14 dated June 9, 2014	Clarification on Proof of Address	Norms for furnishing proof of address have been relaxed to allow submitting only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. It was also advised that in case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months. In case the proof of address

Sr. No.	Circular No. and date	Subject	Gist of instructions
			furnished by the customer is not the local address or address where the customer is currently residing, the bank may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letter, cheque books, ATM cards; (ii) telephonic conversation; (iii) visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.
69	DBOD.AML.BC.No.124/14.01.001/2013-14 dated June 26, 2014	Unique Customer Identification Code (UCIC) for banks' customers in India	In view the requests received, from banks for allowing more time to complete the exercise of allotting UCIC to existing customers, it was decided to extend the time for completing the process of allotting UCIC to existing customers up to December 31, 2014.
70	DBOD.AML.BC.No.26/14.01.001/2014-15 dated July 17, 2014	Amendment to Prevention of Money-laundering (Maintenance of Records) Rules Notified in 2013	KYC/AML/CFT instructions issued to Reporting entities were revised in view of the amendment to PML Rules, notified on August 27, 2013.
71	DBOD.AML.BC.No.39/14.01.001/2014-15 dated September 4, 2014	KYC/AML/CFT Norms - Client Due Diligence measures	It was decided to dispense with the requirement of 'positive confirmation' while periodically updating Client Due Diligence

Sr. No.	Circular No. and date	Subject	Gist of instructions
			measures. It was also advised that physical presence of the customers may, however, not be insisted upon at the time of such periodic updations
72	DBOD.AML.BC.No.44/14.01.001/2014-15 dated October 21, 2014	Clarifications on periodic updation of low risk customers, non-requirement of repeated KYC for the same customer to open new accounts and partial freezing of KYC non-compliant accounts	Banks were advised not to seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised as 'low risk', to obtain a self-certification by the customer in case of no change in status with respect to their identities and addresses. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Banks may not insist on physical presence of such low risk customer at the time of periodic updation. If an existing KYC compliant customer of a bank desires to open another account in the same bank, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose. In cases of non-compliance of KYC requirements by the customers despite repeated reminders by banks, banks were allowed to impose 'partial freezing' on such KYC non-compliant in a phased manner, after giving due notice.
73	DBR.AML.BC.No.77/14.01.001/2014-15 dated March 13, 2015	Know your Customer (KYC) guidelines – in respect of accounts	With a view to ease the process of opening bank accounts of proprietary concerns while keeping the default rule for

Sr. No.	Circular No. and date	Subject	Gist of instructions
		of proprietary concerns	submitting any two documents as activity proof by a proprietary concern, it was allowed that in cases where the banks are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the banks, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern. It was further clarified that the list of registering authorities indicated in the Master circular is only illustrative and includes license/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute, as one of the documents to prove the activity of the proprietary concern.
74	DBR.AML.BC.No.104/14.01.001/2014-15 dated June 11, 2015	Amendment to Prevention of Money Laundering (Maintenance of Records) Rules, 2005 – additional documents for the limited purpose of 'proof of address'	Based on the amendments to PML Rules notified vide Government of India's Gazette Notification dated April 15, 2015, banks/financial institutions were advised about certain additional documents for the limited purpose of proof of address under 'simplified measures'.

A. List of Circulars consolidated in the Master Circular for UCBs

Sr. No.	Circular No.	Date	Subject
1.	UBD.BPD.Cir.No.25/14.01.062/2014-15	08.04.2015	Anti Money Laundering(AML) /Combating of Financing of Terrorism (CFT-Standards-UCBs/StCBs/DCCBs
2.	DCBR.BPD.(PCB/RCB).Cir.No.24/14.01.062/2014-15	01.04.2015	Know your Customer (KYC) guidelines - accounts of proprietary concerns
3.	DCBR.CO.BPD(RCB)Cir. No.9/14.062/014-15	07.01.2015	Designed Director-Amendment to Section 13(2) of Prevention of Money Laundering Act (PMLA)2002
4.	DCBR.CO.BPD.(AD).Cir.No.1/14.062/014-15	13.11.2014	Anti Money Laundering(AML)/ Combating of Financing of Terrorism (CFT-Standards-UCBs
5.	DCBR.CO.BPD.(PCB).No.1/14.01.062/2014-15	05.11.2014	Designed Director-Amendment to Section 13(2) of Prevention of Money Laundering Act (PMLA)
6	UBD.BPD.(PCB).Cir.No.23/14.01.062/2014-15	22.10.2014	Know your Customer (KYC) Norms/ Anti Money Laundering(AML)/Combating of Financing of Terrorism (CFT) Guidelines
7	UBD.BPD.(PCB).Cir.No.22/14.01.062/2014-15	22.10.2014	Know your Customer (KYC) Norms-Clarification on Proof of address
8	UBD.BPD.(PCB).Cir.No.16/14.01.062/2014-15	16.09.2014	Simplification of KYC Norms - Creating Public Awareness
9	UBD.BPD(PCB).Cir.No.15/14.01.062/2014-15	16.09.2014	Client Due Diligence measures
10	UBD.BPD.(PCB).Cir.No.5/14.01.062/2014-15	05.08.2014	Amendment to Prevention of Money-laundering (Maintenance of Records) Rules 2013
11	UBD.BPD.(AD).Cir.No.1/14.062/2014-15	31.07.2014	Anti Money Laundering(AML)/ Combating of Financing of Terrorism (CFT)/Obligation of Banks
12	UBD.BPD.(PCB).Cir.No.2/14.01. 062/2014-15	02.07.2014	Unique Customer Identification Code (UCIC) for banks'

			customers in India
13	UBD.BPD.(PCB)Cir.No.69/14.01.062/2013-14	10.06.2014	Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT) /Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002 - Clarification on Proof of Address - Primary (Urban) Co-operative Banks
14	UBD.BPD.(PCB).Cir.No.9/14.01.062/2013-14	26.05.2014	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards /Combating of Financing of Terrorism (CFT) / Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002 - Harmonization of KYC Norms for Foreign Portfolio Investors (FPIs) - Primary (Urban) Co-operative Banks
15	UBD.BPD.(PCB).Cir.No.54/14.01.062/2013-14	07.04.2014	Reporting of Cross Border Wire Transfer Report on FINnet Gateway - Primary (Urban) Co-operative Banks
16	UBD.BPD.(PCB).Cir.No.50/14.01.062/2013-14	06.03.2014	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002 - Recognising e-Aadhaar as an 'Officially Valid Document' under PML Rules - Primary (Urban) Co-operative Banks
17	UBD.BPD.(PCB).Cir.No.48/14.01.062/2013-14	18.02.2014	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML)Standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002 -Amendment to Section 13(2) - Primary (Urban) Co-operative Banks
18	UBD.BPD.(PCB).Cir.No.32/1	22.10.2013	Know Your Customer (KYC) /

	4.01.062/2013-14		Anti Money Laundering (AML) Standards /Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002 - 'At par' Cheque Facility extended to Cooperative Banks by Scheduled Commercial Banks
19	UBD.BPD.(PCB).Cir.No.15/14.01.062/2013-14	17.09.2013	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards /Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention ofMoney Laundering Act (PMLA), 2002 - e-KYC Service of UIDAI – Recognising on-line Aadhaar Authentication (Electronic Verification Process) to be accepted as an 'Officially Valid Document' under PML Rules - Primary (Urban) Co-operative Banks
20	UBD.BPD(AD).Cir.No.4/14.01.062/2013-14	10.09.2013	KYC Procedure for Opening of Bank Accounts - Foreign Students Studying in India - Primary (Urban) Co-operative Banks - Primary (Urban) Co-operative Banks
21	UBD.BPD.(PCB).Cir.No.11/14.01.062/2013-14	05.09.2013	Know Your Customer (KYC) / Anti Money Laundering (AML)Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002 – Information Sought by Banks from Customers - Primary (Urban) Co-operative Banks
22	UBD.BPD.(PCB).Cir.No.2/14.01.062/2013-14	31.07.2013	Know Your Customer (KYC) / Anti Money Laundering (AML) Standards /Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002 - Simplifying Norms for Periodical Updation of KYC -

			Primary (Urban) Co-operative Banks
23	UBD.BPD(PCB)Cir.No.54/14.01.062/2012-13	06.06.2013	Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT) Guidelines - Unique Customer Identification Code(UCIC) for Banks' Customers in India - Primary (Urban) Co-operative Banks
24	UBD.BPD(PCB)Cir.No.46/14.01.062/2012-13	03.04.2013	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML)Measures / Combating of Financing of Terrorism (CFT) / Obligations of Banks under Prevention of Money Laundering Act (PMLA), 2002Simplifying Norms for Self Help Groups - Primary (Urban) Co-operative Banks
25	UBD.BPD(PCB)Cir.No.39/14.01.062/2012-13	07.03.2013	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Measures /Combating of Financing of Terrorism (CFT) / Obligations of Banks under Prevention of Money Laundering Act (PMLA), 2002 - Primary (Urban) Co-operative Banks
26	UBD.CO.PCB.Cir.No.37/14.01.062/2012-13	25.02.2013	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML)Measures - Combating of Financing of Terrorism (CFT) / Obligations of Banks under Prevention of Money Laundering Act (PMLA), 2002
27	UBD.BPD(PCB)Cir.No.34/14.01.062/2012-13	28.01.2013	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML)Measures / Combating of Financing of Terrorism (CFT) / Obligations of Banks under Prevention of Money Laundering Act (PMLA), 2002
28	UBD.BPD(PCB)Cir.No.28/14.01.062/2012-13	19.12.2012	Know Your Customer (KYC) norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) /

			Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002
29	UBD.BPD.(PCB).Cir.No.14/14.01.062/2012-13	09.10.2012	Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT) Guidelines - Unique Customer Identification Code(UCIC) for banks' customers in India - Primary (Urban) Co-operative Banks
30	UBD.BPD.(PCB).Cir.No.8/14.01.062/2012-13	13.09.2012	Know Your Customer (KYC) / Anti-Money Laundering (AML) /Combating of Financing of Terrorism (CFT) - Risk Categorization and Updation of Customer Profiles - Primary (Urban) Co-operative Banks
31	UBD.CO.BPD(PCB).No.34/12.05.001/2011-12	11.05.2012	Know Your Customer (KYC) Guidelines - Accounts of Proprietary Concerns
32	UBD.CO.BPD.No.24/12.05.001/2011-12	05.03.2012	Know Your Customer (KYC) norms / Anti Money Laundering Standards / Combating of Financing of Terrorism (CFT) / Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002- Assessment and monitoring of risk
33	UBD.BPD.(PCB).Cir.No.20/14.01.062/ 2011-12	01.03.2012	Implementation of Section 51A of UAPA, 1967 - Splitting of UNSC 1267 Committee's list of individuals and entities linked to Al Qaida and Taliban
34	UBD.CO.BPD.No.10/12.05.001/2011-12	09.11.2011	Prevention of Money Laundering Act, 2002 (PMLA) and Rules thereunder - Reporting of CTR, STR etc. to FIU-India- Reporting format under project FINnet
35	UBD.BPD.PCB.No.8/12.05.001/2011-12	09.11.2011	Know Your Customer Norms - Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhar number
36	UBD.CO.BPD.(PCB).Cir.No.9	02.05.2011	Anti-Money Laundering (AML)

	/14.01.062/2010-11		Standards / Combating Financing of Terrorism (CFT) -Standards - Primary (Urban) Co-operative Banks
37	UBD.CO.BPD.(PCB).Cir.No.8 /14.01.062/2010-11	02.05.2011	Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) - Standards - Primary (Urban) Co-operative Banks
38	UBD.CO.BPD.(PCB).Cir.No.7 /14.01.062/2010-11	17.03.2011	Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT)
39	UBD.CO.BPD.(PCB)Cir.No.6/ 14.01.062/2010-11	17.03.2011	Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) – Standards
40	UBD.BPD (PCB) No.38/ 12.05.001/2010-11	15.03.2011	Amendments to Prevention of Money Laundering Rules, 2005
41	UBD.BPD(PCB).No.37/12.05. 001/2010-11	18.02.2011	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
42	UBD.CO.BPD.No.35/12.05.0 01/2010-11	10.01.2011	Opening of bank accounts - Salaried employees
43	UBD.BPD.(PCB).No.32/12.05 .001/2010-11	28.12.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
44	UBD.BPD.(PCB).Cir.No.17/1 4.01.062/2010-11	25.10.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering Standards (AML) / Combating Financing of Terrorism
45	UBD.BPD.(PCB).Cir.No.12/1 2.05.001/2010-11	15.09.2010	Prevention of Money Laundering (Maintenance of the 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) Second Amendment Rules, 2010 - Obligation of banks
46	UBD.BPD.(PCB)No.11/12.05.001/2010-11	25.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
47	UBD.BPD.(PCB).No.10/12.05.001/2010-11	23.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
48	UBD.BPD.(PCB).No.9/12.05.001/2010-11	23.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
49	UBD.BPD.(PCB).Cir.No.7/14.01.062/2010-11	12.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering Standards (AML) / Combating Financing of Terrorism
50	UBD.BPD(PCB).Cir.No.71/12.05.001/2009-10	15.06.2010	Prevention of Money Laundering (Maintenance of the 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) Amendment Rules, 2010 - Obligation of banks / All India Financial Institutions
51	UBD.BPD.CO.53/14.01.062/2009-2010	01.04.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering Standards (AML) / Combating Financing of Terrorism

52	UBD.BPD.(PCB).Cir.No.41/12.05.001/2009-10	03.02.2010	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) Amendment Rules, 2009 - Obligation of banks / Financial institutions
53	UBD.BPD.CO.NSB1/38/1203.000/2009-10	23.12.2009	Know Your Customer (KYC) Guidelines - Accounts of Proprietary Concern
54	UBD.(PCB).CO.BPD.Cir.No.36/14.01.062/2009-10	18.12.2009	Know Your Customer (KYC) Norms / Anti Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)
55	UBD.(PCB).CO.BPD.Cir.No.35/14.01.062/2009-10	17.12.2009	Know Your Customer (KYC) Norms / Anti Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)
56	UBD.(PCB).CO.BPD.Cir.No.33/14.01.062/2009-10	17.12.2009	Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)
57	UBD.CO.BPD.PCB.Cir.No.23/12.05.001/2009-10	16.11.2009	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002 - Urban Cooperative Banks
58	UBD.CO.BPD.PCB.Cir.No.21/12.05.001/2009-10	16.11.2009	Combating Financing of Terrorism - Unlawful Activities (Prevention) Act, 1967 - Obligation of Banks - Urban Cooperative Banks
59	UBD.BPD.CO./NSB1/11/12.03.000/2009-10	29.09.2009	Know Your Customer (KYC) Guidelines - Accounts of Proprietory Concern
60	UBD.CO.BPD.PCB.Cir.No.9/12.05.001/2009-10	16.09.2009	Adherence to KYC / AML guidelines while opening and

			conduct of the accounts of Multi Level Marketing Firms
61	UBD.CO.BPD(PCB).No.1/12.05.001/2008-09	02.07.2008	Prevention of Money Laundering Act, 2002 - Obligation of banks in terms of Rules notified thereunder – UCBs
62	UBD.CO.BPD.(PCB).No.32/09.39.000/2007-08	25.02.2008	Know Your Customer (KYC) Norms / Ant-Money Laundering (AML) Standards / Combating of Financing of Terrorism
63	UBD.CO.BPD.(PCB).No.45/12.05.001/2006-07	25.05.2007	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) Wire Transfers
64	UBD.BPD.Cir.No.38./09.16.100/ 2005-06	21.03.2006	Prevention of Money Laundering Act, 2002 - Obligation of banks in terms of Rules notified thereunder – UCBs
65	UBD.BPD.PCB.Cir.11/09.161.00/ 2005-06	23.08.2005	Know Your Customer Guidelines - Anti-Money laundering Standards - UCBs
66	UBD.PCB.Cir.No.6/09.161.00/2005-06	03.08.2005	Facilitating opening of bank accountsfor flood affected persons
67	UBD.PCB.Cir.30/09.161.00/2004-05	15.12.2004	Know Your Customer (KYC) Guidelines - Anti-Money Laundering Standards - UCBs
68	UBD.BPD.PCB.Cir.02/09.161.00/ 2004-05	09.07.2004	'Know Your Customer' Guidelines – Compliance
69	UBD.BPD.PCB.Cir.48/09.161.00/2003-04	29.05.2004	'Know Your Custmer' Guidelines – Compliance
70	UBD.No.BPD.PCB.Cir.41/09.161.00/2003-04	26.03.2004	'Know Your Customer' Guidelines – Compliance
71	UBD.No.DS.PCB.Cir.17/13.01.00/2002-03	18.09.2002	Guidelines on 'Know Your Customer 'Norms and 'Cash Transactions

List of Circulars consolidated in the Master Circular RPCD.RRB.RCB.AML.BC.No.02/07.51.018/2014-15 dated July 1, 2014 for DCCBs & StCBs

Sr. No.	Circular No.	Date	Subject
1	RPCD.RRB.RCB.AML.No.4424 /07.51.018/2014-15	31.10.2014	KYC - Clarification on Proof of Address
2	RPCD.RRB.RCB.AML.BC.No.3 9/07.51.018/2014-15	31.10.2014	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) Guidelines - Clarifications on Periodic Updation of Low Risk Customers, Non-Requirement of Repeated KYC for the Same Customer to Open New Accounts and Partial Freezing of KYC Non-Compliant Accounts
3	RPCD.RRB.RCB.AML.No.2797 /07.51.018/2014-15	09.09.2014	Simplification of KYC Norms - Creating Public Awareness
4	RPCD.RRB.RCB.AML.BC.No.3 1/07.51.018/2014-15	09.09.2014	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) / Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002 - Client Due Diligence measures
5	RPCD.RRB.RCB.AML.BC.No.1 4/07.51.018/2014-15	21.7.2014	Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under PMLA, 2002 – Amendment to Prevention of Money-Laundering (Maintenance of Records) Rules 2013
6	RPCD.RRB.RCB.AML.BC.No.1 2/07.51.018/2014-15	03.07.2014	Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT) Guidelines -

			Unique Customer Identification Code (UCIC) for Banks' Customers in India
7	RPCD.RRB.RCB.AML.BC.No. 112/07.51.018/2013-14	16.06.2014	Harmonization of KYC norms for Foreign Portfolio Investors (FPIs)
8	RPCD.RRB.RCB.AML.BC.No. 111/07.51.018/2013-14	12.06.2014	Clarification on Proof of address
9	RPCD.RRB.RCB.AML.BC.No. 97/07.51.018/2013-14	25.04.2014	Reporting of Cross Border Wire Transfer Report on FINnet Gateway
10	RPCD.RRB.RCB.AML.BC.No. 92/07.51.018/2013-14	13.03.2014	Recognising e- Aadhaar as an 'Officially Valid Document' under PML Rules
11	RPCD.RRB.RCB.AML.BC.No. 75/07.51.018/2013-14	09.01.2014	Amendment to Section 13(2) of PMLA 2002
12	RPCD.CO.RRB.RCB.BC.No. 48/07.51.010/2013-14	29.10.2013	'At par' cheque facility extended to Cooperative Banks / Regional Rural Banks by Scheduled Commercial Banks
13	RPCD.RRB.RCB.AML.BC.No. 37/07.51.018/2013-14	18.09.2013	Foreign students studying in India
14	RPCD.RRB.RCB.AML.BC.No. 31/07.51.018/2013-14	16.09.2013	Information sought by banks from customers
15	RPCD.RRB.RCB.AML.BC.No. 32/07.51.018/2013-14	10.09.2013	e-KYC Service of UIDAI - Recognising on-line Aadhaar authentication (electronic verification process) to be accepted as an 'Officially Valid Document' under PML Rules
16	RPCD.RRB.RCB.BC.No.84/ 07.51.018/2013-14	25.07.2013	Simplifying norms for periodical updation of KYC
17	RPCD.RCB.RRB.AML.BC.No. 76/07.51.018/2012-13	04.06.2013	Unique Customer Identification Code (UCIC) for banks' customers in India
18	RPCD.RCB.RRB.AML.BC.No. 71/07.51.018/2012-13	01.04.2013	Simplifying Norms for Self Help Groups
19	RPCD.RRB.RCB.BC.No.63/ 07.51.018/2012-13	30.01.2013	Shifting of bank accounts to another centre-address proof
20	RPCD.RRB.RCB.BC.No.59/ 07.51.018/2012-13	22.01.2013	Identification of beneficial owner
21	RPCD.CO.RRB.RCB.AML.No. 6097/ 7.51.018/2012-13	13.12.2012	Simplification of KYC documents
22	RPCD.CO.RRB.RCB.AML.BC. No.36/03.05.33(E)/2012-13 @1	15.10.2012	Uploading of reports on FINnet Gateway
23	RPCD.CO.RRB.RCB.AML.BC. No.29/03.05.33(E)/2012-13	18.09.2012	Uploading of reports in 'Test Mode' on FINnet Gateway

24	RPCD.CO.RRB.RCB.AML.BC. No.82/03.05.33(E)/2011-12	11.06.2012	Unique Customer Identification Code for bank customers in India
25	RPCD.CO.RRB.RCB.AML.BC. No.81/07.40.00/2011-12	11.06.2012	Risk Categorisation and updation of Customer Profile
26	RPCD.CO.RRB.RCB.AML.BC. No.70/07.40.00/2011-12	18.04.2012	Accounts of proprietary concerns
27	RPCD.CO.RCB.AML.BC.No.52 /07.40.00/2011-12	04.01.2012	Splitting of UNSC 1267 Committee's list of individuals and entities linked to Al-Qaida and Taliban
28	RPCD.CO.RRB.AML.BC.No.51 /03.05.33(E)/2011-12	02.01.2012	Splitting of UNSC 1267 Committee's list of individuals and entities linked to Al-Qaida and Taliban
29	RPCD.CO.RCB.AML.BC.No. 50/07.40.00/2011-12	30.12.2011	Assessment and Monitoring of Risk
30	RPCD.CO.RRB.AML.BC.No.46 /03.05.33(E)/2011-12	21.12.2011	Assessment and Monitoring of Risk
31	RPCD.CO.RRB.AML.BC.NO.3 1/03.05.33(E)/2011-12	16.11.2011	Payment of Cheques / Drafts / Pay Orders / Banker's Cheques
32	RPCD.CO.RCB.AML.BC.No.23 /07.40.00/2011-12	17.10.2011	Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number
33	RPCD.CO.RRB.AML.BC.No.21 /03.05.33(E)/2011-12	13.10.2011	Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number
34	RPCD.CO.RRB.AML.BC.No.15 /03.05.33(E)/2011-12	08.08.2011	Opening of "Small Account"
35	RPCD.CO.RCB.AML.BC.No.63 /07.40.00/2010-11	26.04.2011	Opening of "Small Account"
36	RPCD.CO.RCB.AML.BC.No.50 /07.40.00/2010-11	02.02.2011	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'.
37	RPCD.CO.RRB.AML.BC.No.46 /03.05.33(E)/2010-11	12.01.2011	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'.
38	RPCD.CO.RCB.AML.BC.No.39 /07.40.00/2010-11	27.12.2010	Operation of bank accounts & money mules
39	RPCD.CO.RRB.AML.BC.No.40	24.12.2010	Operation of bank accounts &

	/03.05.33(E)/2010-11		money mules
40	RPCD.CO.RCB.AML.BC.No.37 /07.40.00/2010-11	10.12.2010	Opening of bank accounts - salaried employees
41	RPCD.CO.RRB.AML.BC.No.31 /03.05.33(E)/2010-11	06.12.2010	Opening of bank accounts - salaried employees
42	RPCD.CO.RF.AML.BC.No.20/ 07.40.00/2010-11	13.09.2010	Accounts of proprietary concerns
43	RPCD.CO.RRB.AML.BC.No.19 /03.05.33(E)/2010-11	09.09.2010	Accounts of proprietary concerns
44	RPCD.CO.RF.AML.BC.No.12/ 4007.40.00/2010-11	20.07.2010	Prevention of Money Laundering (Maintenance of records of the ... Intermediaries) Second Amendment Rules 2010
45	RPCD.CO.RRB.AML.BC.No.13 /03.05.33(E)/2010-11	22.07.2010	Know Your Customer (KYC) Norms / Anti- Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002
46	RPCD.CO.RF.AML.BC.No.11/ 07.40.00/2010-11	20.07.2010	Obligation of banks under PMLA, 2002
47	RPCD.CO.RF.AML.BC.No.89/ 07.40.00/2009-10	25.06.2010	Client Accounts opened by professional intermediaries
48	RPCD.CORRB.AML.BC.No.87/ 03.05.33(E)/2009-10	23.06.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002
49	RPCD.CO.RF.AML.BC.No.88/ 07.40.00/2009-10	25.06.2010	Filing of STRs; PEPs and Principal Officer
50	RPCD.CO.RRB.AML.BC.No.86 /03.05.33(E)/2009-10	21.06.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002
51	RPCD.CO.RF.AML.BC.No.84/ 07.40.00/2009-10	14.05.2010	Government of India Notification dated February 12, 2010 amending the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005

52	RPCD.CO.RF.AML.BC.No.83/ 07.40.00/2009-10	12.05.2010	Customer identification procedure issued for account opening by proprietary concerns.
53	RPCD.CO.RRB.AML.No.67/ 03.05.33(E)/2009-10	09.04.2010	Know Your Customer (KYC) Guidelines - Accounts of Proprietary Concerns
54	RPCD.CO.RF.AML.BC.No.83/ 07.40.00/2009-10 @2	03.03.2010	Prevention of Money laundering (Amendment) Rules 2009- Obligation of banks / Financial Institutions
55	RPCD.CO.RRB.No.39/03.05.3 3(E)/2009-10	05.11.2009	Combating Financing of Terrorism - Unlawful Activities (Prevention) Act, 1967 - Obligation of Banks
56	RPCD.CO.RF.AML.BC. No.34/07.40.00/2009-10	29.10.2009	Combating Financing of Terrorism- Unlawful Activities (Prevention) Act,(UAPA) 1967- Obligation of banks
57	RPCD.CO.RF.AML. BC.No.28/07.40.00/2009-10	30.09.2009	KYC norms / AML standards / CFT / Obligation of banks under PMLA, 2002
58	RPCD.CO.RRB.BC.No.27/ 03.05.33(E)/2009-10	29.09.2009	Know Your Customer (KYC) Norms / Anti- Money Laundering (AML) Standards and Obligation of Regional Rural Banks (RRBS) Under PMLA, 2002
59	RPCD.CO.RCB.AML.BC.No.81 /07.40.00/2007-08	25.06.2008	Prevention of Money Laundering Act, 2002 - Obligation of banks in terms of Rules notified thereunder.
60	RPCD.CO.RRB.No.BC.77/ 03.05.33(E)/2007-08	18.06.2008	Prevention of Money Laundering Act, 2002 - Obligation of Banks in terms of Rules Notified there under
61	RPCD.CO.RF.AML. BC.No.51/07.40.00/2007-08	28.02.2008	Know Your Customer (KYC) Norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)
62	RPCD.CO.RRB.No.BC.50/03.0 5.33(E)/2007-08	27.02.2008	Know Your Customer (KYC) Norms / Anti- Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)- RRBs
63	RPCD.CO.RRB.AML.BC.No.98 /03.05.28-A/2006-07	21.05.2007	Wire Transfers - Regional Rural Banks (RRBs)
64	RPCD.CO.RF.AML.BC.No.96/	18.05.2007	Wire transfers

	07.40.00/2006-07		
65	RPCD.CO.RRB.AML.BC.68/ 03.05.33(E)/2005-06	09.03.2006	Prevention of Money Laundering Act, 2002 - Obligation of Regional Rural Banks in terms of Rules notified thereunder
66	RPCD.CO.RF.AML.BC.No.65/ 07.40.00/2005-06	03.03.2006	Prevention of Money Laundering Act, 2002 - Obligation of banks in terms of Rules notified thereunder
67	RPCD.No.RRB.BC.33/03.05.33 (E)/2005-06	23.08.2005	Know Your Customer Guidelines - Anti-Money Laundering Standards
68	RPCD.RF.AML.BC.No.30/ 07.40.00/2005-06 @3	23.08.2005	Know Your Customer Guidelines - Anti-Money Laundering Standards
69	RPCD.AML.BC.No.80/07.40.00 /2004-05	18.02.2005	Know Your Customer (KYC) guidelines - Anti Money Laundering Standards
70	RPCD.No.RRB.BC.81/03.05.33 (E)/2004-05	18.02.2005	Know Your Customer (KYC) guidelines - Anti Money Laundering Standards

--------*----------*----------*----------*----------

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/DBR/2015-16/18
Master Direction DBR.AML.BC.No.81/14.01.001/2015-16

February 25, 2016
(Updated as on April 01, 2020)
(Updated as on January 09, 2020)
(Updated as on August 09, 2019)
(Updated as on May 29, 2019)

Master Direction - Know Your Customer (KYC) Direction, 2016

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. [1]REs shall take steps to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of such amendment(s).

2. Accordingly, in exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act *ibid,* Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

CHAPTER – I
PRELIMINARY

1. Short Title and Commencement.

(a) These Directions shall be called the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016.

(b) These directions shall come into effect on the day they are placed on the official website of the Reserve Bank of India.

2. Applicability

(a) The provisions of these Directions shall apply to every entity regulated by Reserve Bank of India, more specifically as defined in 3 (b) (xiii) below, except where specifically mentioned otherwise.

(b) These directions shall also apply to those branches and majority owned subsidiaries of the REs which are located abroad, to the extent they are not contradictory to the local laws in the host country, provided that:

i. where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India.

ii. in case there is a variance in KYC/AML standards prescribed by the Reserve Bank of India and the host country regulators, branches/ subsidiaries of REs are required to adopt the more stringent regulation of the two.

iii. branches/ subsidiaries of foreign incorporated banks may adopt the more stringent regulation of the two i.e. standards prescribed by the Reserve Bank of India and their home country regulators.

Provided that this rule shall not apply to 'small accounts' referred to in Section 23 of Chapter VI.

3. Definitions

In these Directions, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

i. [2]"Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

ii. "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

iii. [3]"Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

iv. Beneficial Owner (BO)

a. Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b. Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

c. Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. [4]"Certified Copy" - Obtaining a certified copy by the RE shall mean comparing the copy of the proof of possession of Aadhaar number where offline

verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE as per the provisions contained in the Act.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

- authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

vi. “Central KYC Records Registry” (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vii. “Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,
d. the Managing Trustee, if the RE is a trust,
e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
f. a person who holds the position of senior management or equivalent designated as a 'Designated Director’ in respect of Cooperative Banks and Regional Rural Banks.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

viii. [5]"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the RE as per the provisions contained in the Act.

ix. [6]"Digital Signature" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

x. [7]"Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

xi. [8]"Know Your Client (KYC) Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry.

xii. "Non-profit organisations" (NPO) means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

xiii. "Officially Valid Document" (OVD) means the passport, the driving licence, [9]proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. [10]where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
   i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
   ii. property or Municipal tax receipt;
   iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
   iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xiv. [11]"Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

xv. "Person" has the same meaning assigned in the Act and includes:
   a. an individual,
   b. a Hindu undivided family,
   c. a company,
   d. a firm,
   e. an association of persons or a body of individuals, whether incorporated or not,

f. every artificial juridical person, not falling within any one of the above persons (a to e), and

g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xvi. "Principal Officer" means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

xvii. "Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. 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

b. appears to be made in circumstances of unusual or unjustified complexity; or

c. appears to not have economic rationale or *bona-fide* purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

xviii. A 'Small Account' means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 23.

xix. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. opening of an account;

b. deposit, withdrawal, 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;

c. the use of a safety deposit box or any other form of safe deposit;

d. entering into any fiduciary relationship;

e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or

f. establishing or creating a legal person or legal arrangement.

xx. [12]"Video based Customer Identification Process (V-CIP)": a method of customer identification by an official of the RE by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

(b) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. "Common Reporting Standards" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

ii. "Customer" means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

iii. "Walk-in Customer" means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.

iv. [13]"Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.

v. "Customer identification" means undertaking the process of CDD.

vi. "FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

vii. "IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

viii. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

ix. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.

x. “On-going Due Diligence” means regular monitoring of transactions in accounts to ensure that they are consistent with the customers’ profile and source of funds.

xi. “Periodic Updation” means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

xii. “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/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

xiii. “Regulated Entities” (REs) means

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as ‘banks’

b. All India Financial Institutions (AIFIs)

c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

xiv. “Shell bank” means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

xv. “Wire transfer” means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

xvi. “Domestic and cross-border wire transfer”: When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the ‘originator

bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

(c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the [14]Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER – II
General

4. There shall be a Know Your Customer (KYC) policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.

5. The KYC policy shall include following four key elements:

(a) Customer Acceptance Policy;

(b) Risk Management;

(c) Customer Identification Procedures (CIP); and

(d) Monitoring of Transactions

6. Designated Director*:*

(a) A "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board.

(b) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

(c) In no case, the Principal Officer shall be nominated as the 'Designated Director'.

7. Principal Officer:

(a) The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

(b) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

8. Compliance of KYC policy

(a) REs shall ensure compliance with KYC Policy through:

(i) Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.

(ii) Allocation of responsibility for effective implementation of policies and procedures.

(iii) Independent evaluation of the compliance functions of REs' policies and procedures, including legal and regulatory requirements.

(iv) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.

(v) Submission of quarterly audit notes and compliance to the Audit Committee.

(b) REs shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

CHAPTER – III

Customer Acceptance Policy

9. REs shall frame a Customer Acceptance Policy.

10. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, REs shall ensure that:

(a) No account is opened in anonymous or fictitious/benami name.

(b) No account is opened where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

(c) No transaction or account-based relationship is undertaken without following the CDD procedure.

(d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

(e) 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

(f) REs shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.

(g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

(i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

(j) [15]Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

(k) [16]Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

11. Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

CHAPTER – IV

Risk Management

12. For Risk Management, REs shall have a risk based approach which includes the following.

(a) Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception of the RE.

(b) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

Chapter V

Customer Identification Procedure (CIP)

13. REs shall undertake identification of customers in the following cases:

(a) Commencement of an account-based relationship with the customer.

(b) Carrying out any international money transfer operations for a person who is not an account holder of the bank.

(c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

(d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

(e) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(f) When a RE has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

(g) REs shall ensure that introduction is not to be sought while opening accounts.

14. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, REs, shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:

(a) [17]Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

(b) Adequate steps are taken by REs to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

(c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping

requirements in line with the requirements and obligations under the PML Act.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the RE.

Chapter VI

Customer Due Diligence (CDD) Procedure

Part I - Customer Due Diligence (CDD) Procedure in case of Individuals

15. [18]Deleted

16. [19]For undertaking CDD, REs shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the RE:

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a bank or to a RE notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or RE shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the RE.

ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the RE shall carry out offline verification.

iii) an equivalent e-document of any OVD, the RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the RE shall carry out verification through digital KYC as specified under Annex I.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the RE pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, REs shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the RE and such exception handling shall also be a part of

the concurrent audit as mandated in Section 8. REs shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the RE and shall be available for supervisory review.

Explanation 1: RE shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

17. Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP.

ii. the aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

iii. the aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.

iv. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 16 is to be carried out.

vi. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

vii. [20]A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, REs shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

viii. REs shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

18. [21]REs may undertake live V-CIP, to be carried out by an official of the RE, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the RE performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:

- Banks: can use either OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by banks for aiding the V-CIP.
- REs other than banks: can only carry out Offline Verification of Aadhaar for identification.

ii. RE shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. The official of the RE shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The official of the RE shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

vii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

viii. RE shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RE shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

ix. To ensure security, robustness and end to end encryption, the REs shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audiovisual interaction shall be triggered from the domain of the RE itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. REs are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the RE.

xiii. RE shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

xiv. BCs can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a bank official. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

19. [22]Deleted

20. [23]Deleted

21. [24]Deleted

22. Deleted

23. [25]Notwithstanding anything contained in Section 16 and as an alternative thereto, in case an individual who desires to open a bank account, banks shall open a 'Small Account', which entails the following limitations:

i. the aggregate of all credits in a financial year does not exceed rupees one lakh;

ii. the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

iii. the balance at any point of time does not exceed rupees fifty thousand.

[26]Provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Further, small accounts are subject to the following conditions:

(a) The bank shall obtain a self-attested photograph from the customer.

(b) The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

[27]Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

(c) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.

(d) Banks shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.

(e) The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the

account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.

(f) The entire relaxation provisions shall be reviewed after twenty four months.

(g) [28]Notwithstanding anything contained in clauses (e) and (f) above, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.

(h) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established as per Section 16.

(i) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per Section 16.

24. [29]**Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs)**: In case a person who desires to open an account is not able to produce documents, as specified in Section 16, NBFCs may at their discretion open accounts subject to the following conditions:

(a) The NBFC shall obtain a self-attested photograph from the customer.

(b) The designated officer of the NBFC certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) The account shall remain operational initially for a period of twelve months, within which CDD as per Section 16 shall be carried out.

(d) Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.

(e) The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.

(f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.

(g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

25. [30]Deleted.

26. [31]KYC verification once done by one branch/office of the RE shall be valid for transfer of the account to any other branch/office of the same RE, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Part II - CDD Measures for Sole Proprietary firms

27. [32]For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

28. [33]In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

(a) Registration certificate

(b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

(c) Sales and income tax returns.

(d) [34]CST/VAT/ GST certificate (provisional/final).

(e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

(f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

(g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.

(h) Utility bills such as electricity, water, landline telephone bills, etc.

29. In cases where the REs are satisfied that it is not possible to furnish two such documents, REs may, at their discretion, accept only one of those documents as proof of business/activity.

Provided REs undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part III- CDD Measures for Legal Entities

30. [35]For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Certificate of incorporation

(b) Memorandum and Articles of Association

(c) [36]Permanent Account Number of the company

(d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

(e) [37]Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

31. [38]For opening an account of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Registration certificate

(b) Partnership deed

(c) [39]Permanent Account Number of the partnership firm

(d) [40]Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

32. [41]For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Registration certificate

(b) Trust deed

(c) [42]Permanent Account Number or Form No.60 of the trust

(d) [43]Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

33A. [44]For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Resolution of the managing body of such association or body of individuals

(b) [45]Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals

(c) Power of attorney granted to transact on its behalf

(d) [46]Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and

(e) Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.

Explanation: Term 'body of individuals' includes societies.

33B. [47]For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Document showing name of the person authorised to act on behalf of the entity;

(b) Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and

(c) Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

Part IV - Identification of Beneficial Owner

34. For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Rules to verify his/her identity shall be undertaken keeping in view the following:

(a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other

intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Part V - On-going Due Diligence

35. REs shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

36. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

(a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

(b) Transactions which exceed the thresholds prescribed for specific categories of accounts.

(c) High account turnover inconsistent with the size of the balance maintained.

(d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

37. The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

(a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

(b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

38. Periodic Updation

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers as per the following procedure:

(a) REs shall carry out

i. CDD, as specified in Section 16, at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

ii. In case of Legal entities, RE shall review the documents sought at the time of opening of account and obtain fresh certified copies.

[48]Provided, REs shall ensure that KYC documents, as per extant requirements of the Master Direction, are available with them.

(b) REs may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

(c) REs shall ensure to provide acknowledgment with date of having performed KYC updation.

(d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

39. [49]In case of existing customers, RE shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which RE shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the RE shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, RE shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60

owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a RE gives in writing to the RE that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, RE shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the RE till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

Part VI - Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

40. [50]**Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding):** REs shall ensure that the first payment is to be effected through the customer's KYC-complied account with another RE, for enhanced due diligence of non-face-to-face customers.

41. Accounts of Politically Exposed Persons (PEPs)

A. REs shall have the option of establishing a relationship with PEPs provided that:

(a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

(b) the identity of the person shall have been verified before accepting the PEP as a customer;

(c) the decision to open an account for a PEP is taken at a senior level in accordance with the REs' Customer Acceptance Policy;

(d) all such accounts are subjected to enhanced monitoring on an on-going basis;

(e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

(f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

B. These instructions shall also be applicable to accounts where a PEP is the beneficial owner

42. Client accounts opened by professional intermediaries:

REs shall ensure while opening client accounts through professional intermediaries, that:

(a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.

(b) REs shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

(c) REs shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the RE.

(d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of RE, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of RE, the RE shall look for the beneficial owners.

(e) REs shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

(f) The ultimate responsibility for knowing the customer lies with the RE.

B. Simplified Due Diligence

43. [51]**Simplified norms for Self Help Groups (SHGs)**

(a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.

(b) CDD of all the office bearers shall suffice.

(c) No separate CDD as per the CDD procedure mentioned in Section 16 of the MD of the members or office bearers shall be necessary at the time of credit linking of SHGs.

44. Procedure to be followed by banks while opening accounts of foreign students

(a) Banks shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.

i. Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.

ii. Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

(b) The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999.

(c) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

45. Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex III, subject to Income Tax (FATCA/CRS) Rules.

Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annex III will be submitted.

Chapter VII
Record Management

46. The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. REs shall,

(a) maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;

(b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

(c) make available the identification records and transaction data to the competent authorities upon request;

(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

(f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

(g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Chapter VIII

Reporting Requirements to Financial Intelligence Unit - India

47. REs shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

48. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those REs, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

49. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented

transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. REs shall not put any restriction on operations in the accounts where an STR has been filed. REs shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

50. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

Chapter IX

Requirements/obligations under International Agreements

Communications from International Agencies –

51. REs shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

(a) The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

(b) The **"1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.

52. Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated March 14, 2019.

53. In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

54. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated [52]March 14, 2019 (Annex II of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

55. Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

(b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in Section 55 a & b do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

(c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

Chapter X
Other Instructions

56. [53]Secrecy Obligations and Sharing of Information:

(a) Banks shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(c) While considering the requests for data/information from Government and other agencies, banks shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. the interest of bank requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.

(e) NBFCs shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

57. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

REs shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

The 'live run' of the CKYCR would start with effect from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, REs shall take the following steps:

(i) Scheduled Commercial Banks (SCBs) shall invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. SCBs are, however, allowed time upto February 1, 2017 for uploading date in respect of accounts opened during January 2017.

(ii) REs other than SCBs shall upload the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

(iii) Operational Guidelines (version 1.1) for uploading the KYC data have been released by CERSAI. Further, 'Test Environment' has also been made available by CERSAI for the use of REs.

58. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, REs shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

(a) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login --> My Account --> Register as Reporting Financial Institution,

(b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: REs shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

(c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

(d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

(e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

(f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. REs may take note of the following:

i. updated Guidance Note on FATCA and CRS

ii. a press release on 'Closure of Financial Accounts' under Rule 114H (8).

59. Period for presenting payment instruments

Payment of cheques/drafts/pay orders/banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

60. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

61. Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituent shall not be collected. Banks shall, at their option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.

62. (a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by banks and NBFCs.

(b) The banks/NBFCs shall, at their option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

63. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.

Adequate attention shall be paid by REs to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

64. Correspondent Banks

Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions:

(a) Sufficient information in relation to the nature of business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country shall be gathered.

(b) Post facto approval of the Board at its next meeting shall be obtained for the proposals approved by the Committee.

(c) The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.

(d) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers

having direct access to the accounts and is undertaking on-going 'due diligence' on them.

(e) The correspondent bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

(f) Correspondent relationship shall not be entered into with a shell bank.

(g) It shall be ensured that the correspondent banks do not permit their accounts to be used by shell banks.

(h) Banks shall be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

(i) Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

65. Wire transfer

REs shall ensure the following while effecting wire transfer:

(a) All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account.

Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions shall be exempt from the above requirements.

(b) Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.

(c) Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND.

(d) Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

(e) A bank processing as an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer.

(f) The receiving intermediary bank shall transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.

(g) All the information on the originator of wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial authorities on receiving such requests.

(h) Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place at a beneficiary bank.

(i) Beneficiary bank shall report transaction lacking complete originator information to FIU-IND as a suspicious transaction.

(j) The beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the beneficiary shall consider restricting or terminating its business relationship with the ordering bank.

66. Issue and Payment of Demand Drafts, etc.,

Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

67. [54]Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

68. Selling Third party products

REs acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

(a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.

(b) transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

(c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) transactions involving rupees fifty thousand and above shall be undertaken only by:

- debit to customers' account or against cheques; and
- obtaining and verifying the PAN given by the account-based as well as walk-in customers.

(e) Instruction at 'd' above shall also apply to sale of REs' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

69. At-par cheque facility availed by co-operative banks

(a) The 'at par' cheque facility offered by commercial banks to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising therefrom.

(b) The right to verify the records maintained by the customer cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements shall be retained by banks.

(c) Cooperative Banks shall:

i. ensure that the 'at par' cheque facility is utilised only:

a. for their own use,

b. for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,

c. for walk-in customers against cash for less than rupees fifty thousand per individual.

ii. maintain the following:

a. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque,

b. sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

iii. ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved.

70. Issuance of Prepaid Payment Instruments (PPIs):

PPI issuers shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

71. Hiring of Employees and Employee training

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the RE, regulation and related issues shall be ensured.

72. Adherence to Know Your Customer (KYC) guidelines by NBFCs/RNBCs and persons authorised by NBFCs/RNBCs including brokers/agents etc.

(a) Persons authorised by NBFCs/ RNBCs for collecting the deposits and their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to NBFCs/RNBCs.

(b) All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by NBFCs/RNBCs including brokers/agents etc. who are operating on their behalf.

(c) The books of accounts of persons authorised by NBFCs/RNBCs including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

Chapter XI
Repeal Provisions

73. With the issue of these directions, the instructions / guidelines contained in the circulars mentioned in the Appendix, issued by the Reserve Bank stand repealed.

74. All approvals / acknowledgements given under the above circulars shall be deemed as given under these directions.

75. All the repealed circulars are deemed to have been in force prior to the coming into effect of these directions.

[55]Annex I

Digital KYC Process

A. The RE shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the REs.

B. The access of the Application shall be controlled by the REs and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by REs to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.

D. The RE must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the RE shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the RE shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the RE who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Banks may use the services of Business Correspondent (BC) for this process.

Annex II

File No.14014/01/2019/CFT
Government of India
Ministry of Home Affairs
CTCR Division

New Delhi, dated 14 March 2019

ORDER

Subject: - Procedure for implementation of Section 51A of the Unlawful (Prevention) Act, 1967.

The Unlawful Activities (Prevention) Act, 1967 (UAPA) was amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51 A, reads as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to —

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism:

(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under :-

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order. 2007, as may be amended from time to time.

In order to expeditiously and effectively implement the provisions of Section 51A, a procedure was outlined vide this Ministry Order No. 17015/10/2002-IS-VI dated 27.08.2009. After the reorganization of the Divisions in Ministry of Home Affairs, the administration of Unlawful Activities (Prevention) Act, 1967 and the work relating to countering of terror financing has been allocated to the CTCR Division. The order dated 27.8.2009 is accordingly modified as under:

Appointment and communication of details of UAPA Nodal Officers

2. As regards appointment and communication of details of UAPA Nodal Officers-

(i) The UAPA Nodal Officer for CTCR Division would be the Joint Secretary (CTCR), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and jsctcr-mha@gov.in (e-mail id).

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the CTCR Division in MHA.

(iii) The States and UTs should appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the CTCR Division in MHA.

(iv) The CTCR Division in MHA would maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA Nodal Officers. to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA Noda! Officers should be circulated by the Nodal Officer of CTCR Division of MHA in July every year and on every change. Joint Secretary (CTCR) being the Nodal Officer of CTCR Division of MHA, shall cause the amended list of UAPA Noda! Officers to be circulated to the Nodal Officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, CTCR Division and Foreigners Division in MHA,

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The CTCR Division of MHA would forward the designated lists to the UAPA Nodal Officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc.

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., the

Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies requiring them to-

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order, herein after, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., held by such customer on their books to the Joint. Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone or 011-23092736. The particulars apart from being sent by post, should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in.

(iii) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in (ii) above to the UAPA Nodal Officer of the State/UT where the account is held and Regulators and FIU-IND, as the case maybe.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation to the Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in.

(v) The banks, stock exchanges /depositories, intermediaries regulated by SEBI and insurance companies, shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 4(ii) above, CTCR Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals / entities identified by the banks, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and

the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an order to freeze these assets under Section 51A of the UAPA would be issued by the UAPA Nodal Officer of CTCR Division of MHA and conveyed electronically/to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA Nodal Officer of CTCR Division of MHA shall also forward a copy thereof to ail the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/ entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of CTCR Division of MHA shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

The order shall be issued without prior notice to the designated individual/entity.

Regarding financial assets or economic resources of the nature of immovable properties

7. CTCR Division of MHA would electronically forward the designated lists to the UAPA Nodal Officer of all States and UTs with the request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable Properties in their respective jurisdiction.

8. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found. the UAPA Nodal Officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to Joint Secretary (CTCR), Ministry of Home Affairs, immediately within 24 hours at Fax No.011- 23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id jsctcr-mha@gov.in.

9. The UAPA Nodal Officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification would be completed within

a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary (CTCR), Ministry of Home Affairs at the Fax, telephone numbers and also on the e-mail id given below.

10. A copy of this reference should be sent to Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also conveyed over telephone on 01123092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id: jsctcr-mha@gov.in. MHA may also have the verification conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under section 51A of the UAPA would be issued, by the UAPA Nodal Officer of CTCR Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA Nodal Officer of the State/UT.

    The order shall be issued without prior notice to the designated individual/entity.

12. Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of the State / UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State / UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act 1967.

Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons: and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

14. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA Nodal Officer for CTCR Division for freezing of funds or other assets.

15. The UAPA Nodal Officer of CTCR Division of MHA, shall cause the request to be examined, within 5 working days, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officers in Regulators, FIU-IND and to the Nodal Officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

16. Upon receipt of the requests by these Nodal Officers from the UAPA nodal officer of CTCR Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall be issued without prior notice to the designated persons involved.

Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

17. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence. in writing, to the concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT Nodal Officers.

18. The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/ UT Nodal Officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Nodal Officer of CTCR Division of MHA as per the contact details given in paragraph 4 (ii) above, within two working days.

19. The Joint Secretary (CTCR), MHA being the UAPA Nodal Officer for CTCR Division of MHA shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, he shall Pass an order, within 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under

intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the Nodal Officers of States/UTs. However, if it is not possible for any reason to pass an Order unfreezing the assets within 15 working days, the UAPA Nodal Officer of CTCR Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act, 1967.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, 1967 relating to funds, financial assets or economic resources or related services, would be communicated to all the banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all Registrars performing the work of registering immovable properties, through the State/UT Nodal Officer by CTCR Division of MHA.

Regarding prevention of entry into or transit through India

21. As regards prevention of entry into or transit through India of the designated individuals the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

Procedure for communication of compliance of action taken under section 51A

23. The Nodal Officers of CTCR Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

24. All concerned are requested to ensure strict compliance of this order.

(Piyush Goyal)

Joint Secretary to the Government of India

1. Governor, Reserve Bank of India, Mumbai
2. Chairman, Securities & Exchange Board of India, Mumbai
3. Chairman, Insurance Regulatory and Development Authority, Hyderabad.

4. Foreign Secretary, Ministry of External Affairs, New Delhi.
5. Finance Secretary, Ministry of Finance, New Delhi.
6. Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7. Director, Intelligence Bureau, New Delhi.
8. Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
9. Chief Secretaries of all States/Union Territories
10. Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
11. Directors General of Police of all States & Union Territories
12. Director General of Police, National Investigation Agency, New Delhi.
13. Commissioner of Police, Delhi.
14. Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
15. Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance. New Delhi.
16. Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.
17. Director (FIU-IND), New Delhi.

Annex III
KYC documents for eligible FPIs under PIS

		FPI Type		
Document Type		**Category I**	**Category II**	**Category III**
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN [56]	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted *	Exempted *	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution @@	Exempted *	Mandatory	Mandatory
Senior Management (Whole Time Directors/ Partners/ Trustees/ etc.)	List	Mandatory	Mandatory	Mandatory
	Proof of Identity	Exempted *	Exempted *	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

Authorized Signatories	List and Signatures	Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *
Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory (can declare “no UBO over 25%”)	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

* Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank.

@@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit ‘Power of Attorney granted to Global Custodian/Local Custodian in lieu of Board Resolution’

Category	Eligible Foreign Investors
I.	Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations/ Agencies.
II.	a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance /Reinsurance Companies, Other Broad Based Funds etc. b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers etc. c) Broad based funds whose investment manager is appropriately regulated. d) University Funds and Pension Funds. e) University related Endowments already registered with SEBI as FII/Sub Account.
III.	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

Appendix

List of Circulars or part thereof repealed with the issuance of Master Direction

Sr.No.	Circular No.	Date
1.	DBOD.BP.BC.92/C.469-76	August 12, 1976
2.	DBOD.GC.BC.62/c.408(A)/87	November 11, 1987
3.	DBOD.BP.BC.114/C.469 (81)-91	April 19, 1991
4.	DBOD.FMC.No.153/27.01.003/93-94	September 1, 1993
5.	DBOD.GC.BC.193/17.04.001/93	November 18, 1993
6.	DBOD.GC.BC.202/17.04.001/93	December 6, 1993
7.	DBOD.No.GC.BC.46/17.04.001	April 22, 1994
8.	DBOD.BP.BC.106/21.01.001/94	September 23,1994
9.	DBOD.BP.BC.102/21.01.001/95	September 20, 1995
10.	DBOD.BP.BC.42/21.01.001/96	April 6, 1996
11.	DBOD.No.BP.BC.12/21.01.023/98	February 11, 1998
12.	DBOD.BP.52/21.01.001/2001-02	December 5, 2001
13.	DBOD.AML.BC.89/14.01.001/2001-02	April 15, 2002
14.	DBOD.AML.BC.No.102/14.01.001/2001-02	May 10, 2002
15.	DBOD.AML.BC.18/14.01.001/2002-03	August 16, 2002
16.	DBOD.NO.AML.BC.58/14.01.001/2004-05	November 29, 2004
17.	DBOD.NO.AML.BC.28 /14.01.001/2005-06	August 23, 2005
18.	DBOD.NO.AML.BC.63/14.01.001/2005-06	February 15, 2006
19.	DBOD.AML.BC. No.77/14.01.001 /2006-07	April 13, 2007
20.	DBOD.AML.BC.No. 63/14.01.001/2007-08	February 18, 2008
21.	DBOD.AML.BC.No. 85/14.01.001/2007 -08	May 22, 2008
22.	DBOD.AML.BC.No.12/14.01.001/2008-09	July 1, 2008
23.	DBOD.AML.BC.No.2/14.01.001/2009-10	July 1, 2009
24.	DBOD.AML.BC.No.43/14.01.001/2009-10	September 11, 2009

25.	DBOD.AML.BC.No.44/14.01.001/2009-10	September 17, 2009
26.	DBOD.AML.BC.No.68/14.01.001/2009-10	January 12, 2010
27.	DBOD.AML.BC.No.80/14.01.001/2009-10	March 26, 2010
28.	DBOD.AML.BC.No.95/14.01.001/2009-10	April 23, 2010
29.	DBOD.AML.BC.No.108/14.01.001/2009-10	June 9, 2010
30.	DBOD.AML.BC.No.109/14.01.001/2009-10	June 10, 2010
31.	DBOD.AML.BC.No.111/14.01.001/2009-10	June 15, 2010
32.	DBOD.AML.BC.No.113/14.01.001/2009-10	June 29, 2010
33.	DBOD.AML.BC.No.38/14.01.001/2010-11	August 31, 2010
34.	DBOD.AML.BC.No.50/14.01.001/2010-11	October 26, 2010
35.	DBOD.AML.BC.No.65/14.01.001/2010-11	December 7, 2010
36.	DBOD.AML.BC.No.70/14.01.001/2010-11	December 30, 2010
37.	DBOD.AML.BC.No.77/14.01.001/2010-11	January 27, 2011
38.	DBOD.AML.BC.No.36/14.01.001/2011-12	September 28, 2011
39.	DBOD.AML BC.No.47/14.01.001/2011-12	November 04, 2011
40.	DBOD. AML.BC.No.65/14.01.001/2011-12	December 19, 2011
41.	DBOD AML BC No.70/14.01.001/2011-12	December 30, 2011
42.	DBOD. AML.BC.No 93/14.01.001/2011-12	April 17, 2012
43.	DBOD. AML.BC.No 109/14.01.001/2011-12	June 08, 2012
44.	DBOD. AML.BC.No 110/14.01.001/2011-12	June 08, 2012
45.	DBOD.AML.BC. No.39/14.01.001/2012-13	September 7, 2012
46.	DBOD.AML.BC. No.49/14.01.001/2012-13	September 7, 2012
47.	DBOD.AML.BC. No.65/14.01.001/2012-13	December 10, 2012
48.	DBOD.AML.BC. No.71/14.01.001/2012-13	January 18, 2013
49.	DBOD.AML.BC. No. 78/14.01.001/2012-13	January 29, 2013
50.	DBOD.AML.BC. No.87/14.01.001/2012-13	March 28, 2013
51.	DBOD. AML.BC. No.101/14.01.001/2011-12	May 31, 2013

52.	DBOD.AML.BC. No.29/14.01.001/2013-14	July 12, 2013
53.	DBOD.AML.BC. No.34/14.01.001/2013-14	July 23, 2013
54.	DBOD.AML.BC.No.44/14.01.001/2013-14	September 2, 2013
55.	DBOD.AML.BC.No.45/14.01.001/2013-14	September 2, 2013
56.	DBOD. AML.BC. No.50/14.01.001/2013-14	September 3, 2013
57.	DBOD.AML.BC.No.63/14.01.001/2013-14	October 29, 2013
58.	DBOD.AML.BC. No.80/14.01.001/2013-14	December 31, 2013
59.	DBOD.AML.BC.No.100/14.01.001/2013-14	March 4, 2014
60.	DBOD. AML. No. 16415/14.01.001/2013-14	March 28, 2014
61.	DBOD.AML.BC.No.103/14.01.001/2013-14	April 3, 2014
62.	DBOD.AML.BC. No. 119/14.01.001/2013-14	June 9, 2014
63.	DBOD. AML.BC. No.124/14.01.001/2013-14	June 26, 2014
64.	DBOD.AML.BC.No.26/14.01.001/2014-15	July 17, 2014
65.	DBOD.AML.BC.No. 39/14.01.001/2014-15	September 4, 2014
66.	DBOD. AML. BC. No.44/14.01.001/2014-15	October 21, 2014
67.	DBR.AML.BC.No.77/14.01.001/2014-15	March 13, 2015
68.	DBR.AML. BC. No.104/ 14.01.001/ 2014-15	June 11, 2015
69.	DBR.AML.BC.No.36/14.01.001/2015-16	August 28, 2015
70.	DBR. AML.BC. No.46/14.01.001/2015-16	October 29, 2015
71.	DBR.AML.BC.No.60/14.01.001/2015-16	November 26, 2015
72.	DBOD.NO.BC.23/21.01.001/92	September 9, 1992
73.	DBOD.BP.BC No.56/21.01.001/2005-06	January 23, 2006
74.	DBOD.BP.BC.No.50/21.01.001/2011-12	November 4, 2011
75.	DBOD.BP.BC.No.87/21.01.001//2013-14	January 22, 2014
76.	DBOD.No.BP.BC.110/21.02.051/98	November 18, 1998
77.	UBD.BPD.(PCB)Cir.No.69/14.01.062/2013-14	June 10, 2014
78.	UBD.BPD.PCB).Cir.No.9/14.01.062/2013-14	May 26, 2014

79.	UBD.BPD.(PCB).Cir.No.54/14.01.062/2013-14	April 7, 2014
80.	UBD.BPD.(PCB).Cir.No.50/14.01.062/2013-14	March 6, 2014
81.	UBD.BPD.(PCB).Cir.No.48/14.01.062/2013-14	February 18, 2014
82.	UBD.BPD.(PCB).Cir.No.32/14.01.062/2013-14	October 22, 2013
83.	UBD.BPD.(PCB).Cir.No.15/14.01.062/2013-14	September 17, 2013
84.	UBD.BPD(AD).Cir.No.4/14.01.062/2013-14	September 10, 2013
85.	UBD.BPD.(PCB).Cir.No.11/14.01.062/2013-14	September 05, 2013
86.	UBD.BPD.(PCB).Cir.No.2/14.01.062/2013-14	July 31, 2013
87.	UBD.BPD(PCB)Cir.No.54/14.01.062/2012-13	June 6, 2013
88.	UBD.BPD(PCB)Cir.No.46/14.01.062/2012-13	April 03, 2013
89.	UBD.BPD(PCB)Cir.No.39/14.01.062/2012-13	March 07, 2013
90.	UBD.CO.PCB.Cir.No.37/14.01.062/2012-13	February 25, 2013
91.	UBD.BPD(PCB)Cir.No.34/14.01.062/2012-13	January 28, 2013
92.	UBD.BPD(PCB)Cir.No.28/14.01.062/2012-13	December 19, 2012
93.	UBD.BPD.(PCB).Cir.No.14/14.01.062/2012-13	October 9, 2012
94.	UBD.BPD.(PCB).Cir.No.8/14.01.062/2012-13	September 13, 2012
95.	UBD.CO.BPD(PCB).No.34/12.05.001/2011-12	May 11, 2012
96.	UBD.CO.BPD.No.24/12.05.001/2011-12	March 5, 2012
97.	UBD.BPD.(PCB).Cir.No.20/14.01.062/ 2011-12	March 01, 2012
98.	UBD.CO.BPD.No.10/12.05.001/2011-12	November 09, 2011
99.	UBD.BPD.PCB.No.8/12.05.001/2011-12	November 9, 2011
100.	UBD.CO.BPD.(PCB).Cir.No.9/ 14.01.062/2010-11	May 2, 2011
101.	UBD.CO.BPD.(PCB).Cir.No.8/ 14.01.062/2010-11	May 2, 2011
102.	UBD.CO.BPD.(PCB).Cir.No.7/14.01.062/2010-11	March 17, 2011
103.	UBD.CO.BPD.(PCB)Cir.No.6/14.01.062/2010-11	March 17, 2011
104.	UBD.BPD (PCB) No.38/12.05.001/2010-11	March 15, 2011
105.	UBD.BPD(PCB).No.37/12.05.001/2010-11	February 18, 2011

106.	UBD.CO.BPD.No.35/12.05.001/2010-11	January 10, 2011
107.	UBD.BPD.(PCB).No.32/12.05.001/2010-11	December 28, 2010
108.	UBD.BPD.(PCB).Cir.No.17/14.01.062/2010-11	October 25, 2010
109.	UBD.BPD.(PCB).Cir.No.12/12.05.001/2010-11	September 15, 2010
110.	UBD.BPD.(PCB)No.11/12.05.001/2010-11	August 25, 2010
111.	UBD.BPD.(PCB).No.10/12.05.001/2010-11	August 23, 2010
112.	UBD.BPD.(PCB).No.9/12.05.001/2010-11	August 23, 2010
113.	UBD.BPD.(PCB).Cir.No.7/ 14.01.062/2010-11	August 12, 2010
114.	UBD.BPD(PCB).Cir.No.71/12.05.001/2009-10	June 15, 2010
115.	UBD.BPD.CO.53/14.01.062/ 2009-2010	April 1, 2010
116.	UBD. BPD. (PCB).Cir. No.41/12.05.001/2009-10	February 3, 2010
117.	UBD.BPD.CO.NSB1/38/1203.000/2009-10	December 23, 2009
118.	UBD.(PCB).CO.BPD.Cir.No.36/14.01.062/2009-10	December 18, 2009
119.	UBD.(PCB).CO.BPD.Cir.No.35/14.01.062/2009-10	December 17, 2009
120.	UBD.(PCB).CO.BPD.Cir.No.33/14.01.062/2009-10	December 17, 2009
121.	UBD.CO.BPD.PCB.Cir.No.23/12.05.001/2009-10	November 16, 2009
122.	UBD.CO.BPD.PCB.Cir.No.21/12.05.001/2009-10	November 16, 2009
123.	UBD.BPD.CO./NSB1/11/12.03.000/2009-10	September 29, 2009
124.	UBD.CO.BPD.PCB.Cir.No.9/12.05.001/2009-10	September 16, 2009
125.	UBD.CO.BPD(PCB).No.1/12.05.001/2008-09	July 2, 2008
126.	UBD.CO.BPD.(PCB).No.32/09.39.000/2007-08	February 25, 2008
127.	UBD.CO.BPD.(PCB).No.45/12.05.001/2006-07	May 25, 2007
128.	UBD.BPD.Cir.No.38./09.16.100/2005-06	March 21, 2006
129.	UBD.BPD.PCB.Cir.11/09.161.00/2005-06	August 23, 2005
130.	UBD.PCB.Cir.No.6/09.161.00/2005-06	August 03, 2005
131.	UBD.PCB.Cir. 30/09.161.00/2004-05	December 15, 2004
132.	UBD.BPD.PCB.Cir.02/09.161.00/2004-05	July 09, 2004

133.	UBD.BPD.PCB.Cir.48/09.161.00/2003-04	May 29, 2004
134.	UBD.No.BPD.PCB.Cir.41/09.161.00/2003-04	March 26, 2004
135.	UBD.No.DS.PCB.Cir.17/13.01.00/2002-03	September 18, 2002
136.	RPCD.RRB.RCB.AML.BC.No.112/07.51.018/2013-14	June 16, 2014
137.	RPCD.RRB.RCB.AML.BC.No.111/07.51.018/2013-14	June 12, 2014
138.	RPCD.RRB.RCB.AML.BC.No.97/07.51.018/2013-14	April 25, 2014
139.	RPCD.RRB.RCB.AML.BC.No.92/07.51.018/2013-14	March 13, 2014
140.	RPCD.RRB.RCB.AML.BC.No.75/07.51.018/2013-14	January 09, 2014
141.	RPCD.CO.RRB.RCB.BC.No.48/07.51.010/2013-14	October 29, 2013
142.	RPCD.RRB.RCB.AML.BC.No.37/07.51.018/2013-14	September 18, 2013
143.	RPCD.RRB.RCB.AML.BC.No.31/07.51.018/2013-14	September 16, 2013
144.	RPCD.RRB.RCB.AML.BC.No.32/07.51.018/2013-14	September 10, 2013
145.	RPCD.RRB.RCB.BC.No.84/07.51.018/2013-14	July 25, 2013
146.	RPCD.RCB.RRB.AML.BC.No.76/07.51.018/2012-13	June 4, 2013
147.	RPCD.RCB.RRB.AML.BC.No.71/07.51.018/2012-13	April 1, 2013
148.	RPCD.RRB.RCB.BC.No.63/07.51.018/2012-13	January 30, 2013
149.	RPCD.RRB.RCB.BC.No.59/07.51.018/2012-13	January 22, 2013
150.	RPCD.CO.RRB.RCB.AML.No.6097/7.51.018/2012-13	December 13, 2012
151.	RPCD.CO.RRB.RCB.AML.BC.No.36/03.05.33(E)/2012-13	October 15, 2012
152.	RPCD.CO.RRB.RCB.AML.BC.No.29/03.05.33(E)/2012-13	September 18, 2012
153.	RPCD.CO.RRB.RCB.AML.BC.No.82/03.05.33(E)/2011-12	June 11, 2012
154.	RPCD.CO.RRB.RCB.AML.BC.No.81/07.40.00/2011-12	June 11, 2012
155.	RPCD.CO.RRB.RCB.AML.BC.No.70/07.40.00/2011-12	April 18, 2012
156.	RPCD.CO.RCB.AML.BC.No.52/07.40.00/2011-12	January 04, 2012
157.	RPCD.CO.RRB.AML.BC.No.51/03.05.33(E)/2011-12	January 02, 2012
158.	RPCD.CO.RCB.AML.BC.No.50/07.40.00/2011-12	December 30, 2011

159.	RPCD.CO.RRB.AML.BC.No.46/03.05.33(E)/2011-12	December 21, 2011
160.	RPCD.CO.RRB.AML.BC.NO.31/03.05.33(E)/2011-12	November 16, 2011
161.	RPCD.CO.RCB.AML.BC.No.23/07.40.00/2011-12	October 17, 2011
162.	RPCD.CO.RRB.AML.BC.No.21/03.05.33(E)/2011-12	October 13, 2011
163.	RPCD.CO.RRB.AML.BC.No.15/03.05.33(E)/2011-12	August 8, 2011
164.	RPCD.CO.RCB.AML.BC.No.63/07.40.00/2010-11	April 26, 2011
165.	RPCD.CO.RCB.AML.BC.No.50/07.40.00/2010-11	February 2, 2011
166.	RPCD.CO.RRB.AML.BC.No.46/03.05.33(E)/2010-11	January 12, 2011
167.	RPCD.CO.RCB.AML.BC.No.39/07.40.00/2010-11	December 27, 2010
168.	RPCD.CO.RRB.AML.BC.No.40/03.05.33(E)/2010-11	December 24, 2010
169.	RPCD.CO.RCB.AML.BC.No.37/07.40.00/2010-11	December 10, 2010
170.	RPCD.CO.RRB.AML.BC.No.31/03.05.33(E)/2010-11	December 6, 2010
171.	RPCD.CO.RF.AML.BC.No.20/07.40.00/2010-11	September 13, 2010
172.	RPCD.CO.RRB.AML.BC.No.19/03.05.33(E)/2010-11	September 9, 2010
173.	RPCD.CO.RF.AML.BC.No.12/4007.40.00/2010-11	July 20, 2010
174.	RPCD.CO.RRB.AML.BC.No.13/03.05.33(E)/2010-11	July 22, 2010
175.	RPCD.CO.RF.AML.BC.No.11/07.40.00/2010-11	July 20, 2010
176.	RPCD.CO.RF.AML.BC.No.89/07.40.00/2009-10	June 25, 2010
177.	RPCD.CORRB.AML.BC.No.87/03.05.33(E)/2009-10	June 23, 2010
178.	RPCD.CO.RF.AML.BC.No.88/07.40.00/2009-10	June 25, 2010
179.	RPCD.CO.RRB.AML.BC.No.86/03.05.33(E)/2009-10	June 21, 2010
180.	RPCD.CO.RF.AML.BC.No.84/07.40.00/2009-10	May 14, 2010
181.	RPCD.CO.RF.AML.BC.No.83/07.40.00/2009-10	May 12, 2010
182.	RPCD.CO.RRB.AML.No.67/03.05.33(E)/2009-10	April 9, 2010
183.	RPCD.CO.RF.AML.BC.No.83/07.40.00/2009-10	March 3, 2010
184.	RPCD.CO.RRB.No.39/03.05.33(E)/2009-10	November 5, 2009

185.	RPCD.CO.RF.AML.BC.No.34/07.40.00/2009-10	October 29, 2009
186.	RPCD.CO.RF.AML.BC.No.28/07.40.00/2009-10	September 30, 2009
187.	RPCD.CO.RRB.BC.No.27/03.05.33(E)/2009-10	September 29, 2009
188.	RPCD.CO.RCB.AML.BC.No.81/07.40.00/2007-08	June 25, 2008
189.	RPCD.CO.RRB.No.BC.77/03.05.33(E)/2007-08	June 18, 2008
190.	RPCD.CO.RF.AML.BC.No.51/07.40.00/2007-08	February 28, 2008
191.	RPCD.CO.RRB.No.BC.50/03.05.33(E)/2007-08	February 27, 2008
192.	RPCD.CO.RRB.AML.BC.No.98/03.05.28-A/2006-07	May 21, 2007
193.	RPCD.CO.RF.AML.BC.No.96/07.40.00/2006-07	May 18, 2007
194.	RPCD.CO.RRB.AML.BC.68/03.05.33(E)/2005-06	March 9, 2006
195.	RPCD.CO.RF.AML.BC.No.65/07.40.00/2005-06	March 3, 2006
196.	RPCD.No.RRB.BC.33/03.05.33(E)/2005-06	August 23, 2005
197.	RPCD.RF.AML.BC.No.30/07.40.00/2005-06	August 23, 2005
198.	RPCD.AML.BC.No.80/07.40.00/2004-05	February 18, 2005
199.	RPCD.No.RRB.BC.81/03.05.33 (E)/2004-05	February 18, 2005
200.	DNBS (PD) CC.No.46/02.02(RNBC)/2004-05	December 30, 2004
201.	DNBS(PD). CC 48/10.42/2004-05	February 21, 2005
202.	DNBS(PD).CC No. 58/10.42/2005-06	October 11, 2005
203.	DNBS.PD. CC No. 64/03.10.042/2005-06	March 7, 2006
204.	DNBS (PD). CC 113/03.10.042/2007- 08	April 23, 2008
205.	DNBS (PD). CC 163/03.10.042/2009- 10	November 13, 2009
206.	DNBS (PD).CC. No 166/03.10.42/2009-10	December 2, 2009
207.	DNBS. (PD) CC No 192/03.10.42/2010-11	August 9, 2010
208.	DNBS. (PD) CC No 193/03.10.42/2010-11	August 9, 2011
209.	DNBS (PD).CC. No 201/03.10.42 /2010-11	September 22, 2010
210.	DNBS (PD).CC. No 202/03.10.42/2010-11	October 4, 2010
211.	DNBS(PD).CC.No209/03.10.42/2010- 11	January 28, 2011

212.	DNBS(PD).CC.No210/03.10.42/2010-11	February 14, 2011
213.	DNBS.(PD)CCNo212/03.10.42/2010-11	March 8, 2011
214.	DNBS(PD).CC. No.216/03.10.42/2010-11	May 2, 2011
215.	DNBS(PD).CC.No218/03.10.42/2010-11	May 4, 2011
216.	DNBS.(PD)CC No215/03.10.42/2010-11	April 5, 2011
217.	DNBS (PD).CC. No 242/03.10.42/2011-12	September 15, 2011
218.	DNBS (PD).CC. No 244/03.10.42/2011-12	September 22, 2011
219.	DNBS (PD).CC. No 251/03.10.42/2011-12	December 26, 2011
220.	DNBS (PD).CC. No 257/03.10.42/2011-12	March 14, 2012
221.	DNBS (PD).CC. No 264/03.10.42/2011-12	March 21, 2012
222.	DNBS(PD).CC. No.270/03.10.42/2011-12	April 4, 2012
223.	DNBS (PD).CC. No 275/03.10.42/2011-12	May 29, 2012
224.	DNBS (PD).CC. No 294/03.10.42/2012-13	July 5, 2012
225.	DNBS (PD).CC. No 295/03.10.42/2012-13	July 11, 2012
226.	DNBS (PD).CC. No 296/03.10.42/2012-13	July 11, 2012
227.	DNBS (PD).CC. No 298/03.10.42/2012-13	July 26, 2012
228.	DNBS (PD).CC. No 302/03.10.42/2012-13	September 7, 2012
229.	DNBS (PD).CC. No 304/03.10.42/2012-13	September 17, 2012
230.	DNBS (PD).CC. No 305/03.10.42/2012-13	October 3, 2012
231.	DNBS (PD).CC. No 306/03.10.42/2012-13	October 3, 2012
232.	DNBS (PD).CC. No 310/03.10.42/2012-13	November 22, 2012
233.	DNBS (PD).CC. No 313/03.10.42/2012-13	December 10, 2012
234.	DNBS (PD).CC. No 318/03.10.42/2012-13	December 28, 2012
235.	DNBS (PD).CC. No 319/03.10.42/2012-13	December 28, 2012
236.	DNBS (PD).CC. No 321/03.10.42/2012-13	February 27, 2013
237.	DNBS (PD).CC. No 323/03.10.42/2012-13	April 18, 2013
238.	DNBS (PD).CC. No 324/03.10.42/2012-13	May 2, 2013

239.	DNBS (PD).CC. No 325/03.10.42/2012-13	May 3, 2013
240.	DNBS(PD).CC.No.351/03.10.42/2013-14	July 4, 2013
241.	DNBS (PD).CC. No 352/03.10.42/2013-14	July 23, 2013
242.	DNBS(PD).CC.No 357/03.10.42/2013-14	October 3, 2013
243.	DNBS(PD).CC NO 358/03.10.42/2013-14	October 3, 2013
244.	DNBS(PD).CC.No.364/03.10.42/2013-14	January 1, 2014
245.	DNBS(PD).CC.No.366/03.10.42/2013-14	January 10, 2014
246.	DNBS (PD).CC. No 370/03.10.42/2013-14	March 19, 2014
247.	DNBS(PD).CC.No.375/03.10.42/2013-14	April 22, 2014
248.	DNBS (PD).CC. No 401/03.10.42/2014-15	July 25, 2014
249.	DNBS (PD).CC. No 402/03.10.42/2014-15	August 1, 2014
250.	DNBS (PD).CC. No 404/03.10.42/2014-15	August 1, 2014
251.	DNBR.CC.PD.No.010/03.10.01/2014-15	January 09, 2015
252.	DNBR(PD).CC.No.034/03.10.42/2014-15	April 30, 2015
253.	DBOD.No.IBS.1816/23.67.001/98-99	February 4, 1999

List of Circulars Repealed Partially, with the issuance of Master Direction

Sr.No.	Circular No.	Date
1.	DBOD.BP.BC.57/21.01.001/95 – Paragraph 2(b)	May 4, 1995
2.	DBS.FGV.BC.56.23.04.001/98-99 Paragraph "(b) Concept of "Know Your Customer" (para. 9.2)"	June 21, 1999

[1] Inserted vide Amendment dated April 20, 2018.
[2] Amended vide amendment dated January 9, 2020.
[3] Amended vide amendment dated May 29, 2019.
[4] Amended vide amendment dated January 9, 2020.
[5] Inserted vide amendment dated January 9, 2020.
[6] Inserted vide amendment dated January 9, 2020.
[7] Inserted vide amendment dated January 9, 2020.
[8] Inserted vide amendment dated January 9, 2020.
[9] Inserted vide amendment dated May 29, 2019.
[10] Amended vide amendment dated January 9, 2020.
[11] Amended vide amendment dated May 29, 2019.
[12] Inserted vide amendment dated January 9, 2020.
[13] Amended vide Gazette Notification G.S.R. 538(E) regarding PML Second amendment Rules dated June 1, 2017. Before amendment, it read as: "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents' as a 'proof of identity' and a 'proof of address".
[14] Inserted vide amendment dated May 29, 2019.
[15] Inserted vide amendment dated January 9, 2020.
[16] Inserted vide amendment dated January 9, 2020.
[17] Amended vide Gazette Notification G.S.R. 544(E) regarding PML Second amendment Rules 2015 dated July 7, 2015. Before amendment, it read as: "Necessary information of such customers' due diligence carried out by the third party is immediately obtained by REs".
[18] Deleted vide amendment dated May 29, 2019.
[19] Amended vide amendment dated January 9, 2020.
[20] Amended vide amendment dated May 29, 2019.
[21] Inserted vide amendment dated January 9, 2020.
[22] Deleted vide amendment dated April 20, 2018. Deleted portion to read as: In case the person who proposes to open an account does not have an OVD as 'proof of address', such person shall provide OVD of the relative as provided at sub-section 77 of Section 2 of the Companies Act, 2013, read with Rule 4 of Companies (Specification of definitions details) Rules, 2014, with whom the person is staying, as the 'proof of address' Explanation: A declaration from the relative that the said person is a relative and is staying with him/her shall be obtained.
[23] Deleted vide amendment dated April 20, 2018. Deleted portion to read as: "In cases where a customer categorised as 'low risk', expresses inability to complete the documentation requirements on account of any reason that the REs consider to be genuine, and where it is essential not to interrupt the normal conduct of business, REs shall, at their option, complete the verification of identity of the customer within a period of six months from the date of establishment of the relationship."
[24] Deleted vide amendment dated April 20, 2018. Deleted portion to read as: In respect of customers who are categorised as 'low risk' and are not able to produce any of the OVDs mentioned at Section 3(a)(vi) of Chapter I and where 'simplified procedure' is applied, REs shall, accept any one document from each of the two additional sets of documents listed under the two provisos of sub-Rule 2(1)(d). *Explanation: During the periodic review, if the 'low risk' category customer for whom simplified procedure is applied, is re-categorised as 'moderate or ''high' risk category, then REs shall obtain one of the six OVDs listed at Section 3(a)(vi) of these Directions for proof of identity and proof of address immediately. In the event such a customer fails to submit such an OVD, REs shall initiate action as envisaged in Section 39 of these Directions*.
[25] Amended vide amendment dated January 9, 2020.
[26] Inserted vide Gazette Notification G.S.R. 1038(E) regarding PML Third amendment Rules dated August 21, 2017.
[27] Inserted vide Gazette Notification G.S.R. 381(E) dated May 28, 2019.
[28] Inserted vide amendment dated March 31, 2020.
[29] Amended vide amendment dated May 29, 2019.
[30] Deleted vide amendment dated April 20, 2018 and shifted to Section 10. Deleted/shifted portion to read as: "If an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise."
[31] Amended vide Gazette Notification G.S.R. 538(E) regarding PML Second amendment Rules dated June 1, 2017. Deleted portion of Section 26 is as follows: "and a self-declaration from the account holder about his/her current address is obtained in such cases.
[32] Amended vide amendment dated May 29, 2019.
[33] Amended vide amendment dated May 29, 2019.

[34] Inserted vide amendment dated April 20, 2018.
[35] Amended vide amendment dated January 9, 2020.
[36] Inserted vide amendment dated May 29, 2019.
[37] Amended vide amendment dated January 9, 2020.
[38] Amended vide amendment dated January 9, 2020.
[39] Inserted vide amendment dated May 29, 2019.
[40] Amended vide amendment dated January 9, 2020.
[41] Amended vide amendment dated January 9, 2020.
[42] Inserted vide amendment dated May 29, 2019.
[43] Amended vide amendment dated January 9, 2020.
[44] Amended vide amendment dated January 9, 2020.
[45] Inserted vide amendment dated May 29, 2019.
[46] Amended vide amendment dated January 9, 2020.
[47] Amended vide amendment dated January 9, 2020.
[48] Inserted vide amendment dated January 9, 2020.
[49] Amended vide amendment dated January 9, 2020.
[50] Amended vide amendment dated January 9, 2020.
[51] Amended vide amendment dated May 29, 2019.
[52] Amended vide amendment dated May 29, 2019.
[53] Amended vide amendment dated May 29, 2019.
[54] Amended vide amendment dated January 9, 2020.
[55] Inserted vide amendment dated January 9, 2020.
[56] Amended vide amendment dated April 20, 2018. Deleted Portion of read as: ‘Card’