यूको बैंक UCO BANK
(भारतसरकारकाउपक्रम)
सम्मानआपकेविश्वासका

प्रधान कार्यालय :
परिचालन एवं सेवाएं विभाग
2, इंडिया एक्सचेंज प्लेस
कोलकाता – 700 001

परिपत्र संख्या
सीएचओ/ओएसडी-केवाईसी एवं एएमएल/94/2024-25
दिनांक: 16-05-2024

भारतसंघ की सभी शाखाओं / कार्यालयों को

विषय: अपने ग्राहक को जानिए (केवाईसी) मानदंडों/ धनशोधन निवारण (एएमएल) मानकों/ आतंकवाद के वित्तपोषण का प्रतिरोध (सिएफटी) पर नीतिगत दिशानिर्देश –पीएमएलए,2002 के तहत बैंकों का दायित्व, वित्तीय वर्ष 2024-25, दिनांक 04.01.2024 तक यथा संशोधित ।

भारत संघ की सभी शाखाओं एवं कार्यालयों का ध्यान हमारे परिपत्र संख्या एचओ/ओएसडी - केवाईसी एंड एएमएल/2023-24/034 दिनांक 12.03.2024 की ओर आकृष्ट किया जाता है जिसके साथ अपने ग्राहक को जानिए (केवाईसी) मानदंडों/ धन शोधन निवारण (एएमएल) मानकों/ आतंकवाद के वित्तपोषण का प्रतिरोध (सिएफटी)-पीएमएलए, 2002, वित्तीय वर्ष 2024-25 के तहत बैंकों के दायित्व पर नीतिगत दस्तावेज संलग्न था।

तदन्तर भारत सरकार और भारतीय रिजर्व बैंक द्वारा दिनांक 04.01.2024 तक जारी निम्नलिखित नवीनतम दिशानिर्देशों का अवलोकन करते हुए उक्त नीति को संशोधित किया गया है ।

1. आरबीआई/डीबीआर/2015-16/18 मास्टर दिशानिदेश डीबीआर.एएमएल.बीसी.नं.81/14.01.001/2015-16 दिनांक 25 फरवरी, 2016 को 04 जनवरी, 2024 तक अद्यतन किया गया है।
2. आरबीआई/2023-24/109/ डीओआर.एएमएल.आरईसी.67/14.06.001/2003-24 दिनांक 06 जनवरी 2024
3. आरबीआई/2023-24/111/डीओआर.एएमएल.आरईसी.69/14.06.001/2023-24 दिनांक 11 जनवरी 2024
4. साइबर सक्षम धोखाधड़ी को रोकने के लिए म्यूल खाता खोलने और परिचालन को रोकने के लिए निर्देशिका पर FIU-IND, वित्त विभाग, वित्त मंत्रालय, भारत सरकार द्वारा दिनांक 26.10.2023 को जारी की गई निर्देश -से संबंधित:-
5. निवेश/अंशकालिक नौकरी/पोंजी योजना घोटालों के माध्यम से धोखाधड़ी/साइबर अपराध पर आरबीआई, पर्यवेक्षण विभाग, केवाईसी एएमएल समूह, केंद्रीय कार्यालय, मुंबई द्वारा 10 अगस्त, 2022 को जारी की गई निर्देशिका।

निदेशक मंडल द्वारा दिनांक 30.03.2024 की बैठक में विधिवत अनुमोदन के पश्चात संशोधित दस्तावेज एतदद्वारा संलग्न हैं।

शाखाओं / कार्यालयों को निर्देश दिए जाते हैं कि वे उक्त नीति दस्तावेज से शब्दश: निदेशित हों तथा उसमें निहित निदेशों का समुचित अनुपालन सुनिश्चित करें ।

सरोज रंजन नायक
(सरोज रंजन नायक)
महाप्रबंधक
परिचालन एवं सेवा विभाग

यूको बैंक / UCO BANK ★ के वाई सी एवं ए एम एल सेक्टर KYC & AML Cell ★ प्रधान कार्यालय, कोलकाता / Head Office, Kolkata

संलग्नक : यथोक्त

यूको बैंक UCO BANK
(भारतसरकारकाउपक्रम)
सम्मानआपकेविश्वासका

प्रधान कार्यालय :
परिचालन एवं सेवाएं विभाग
2, इंडिया एक्सचेंज प्लेस
कोलकाता – 700 001

परिपत्र संख्या
सीएचओ/ओएसडी-केवाईसी एवं एएमएल/94/2024-25
दिनांक: 16-05-2024

सभीशाखाओं / कार्यालयोंको
TO ALL THE BRANCHES/OFFICES IN INDIAN UNION:

विषय/Sub: Policy on Know your Customer (KYC) norms/Anti Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)- Obligations of Banks under PMLA, 2002 as amended up to 04.01.2024, FY 2024-25

Attention of all the branches and offices in Indian Union is invited to our Circular No. CHO/OSD-KYC&AML/034/2023-24 dated 12.03.2024 enclosing therewith the Policy Document on Know Your Customer (KYC) norms/Anti Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT) –Obligation of Banks under PMLA, 2002, for FY 2024-25.

The stated policy has since been reviewed and revised by incorporating the following latest guidelines as issued by Govt. Of India & Reserve Bank of India up to 04.01.2024:

1. RBI/DBR/2015-16/18Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25,2016 updated as on January 04, 2024.
2. RBI/2023-24/109/ DOR.AML.REC.67/14.06.001/2003-24 dated January 06, 2024.
3. RBI/2023-24/111/DOR.AML.REC.69/14.06.001/2023-24 dated January 11, 2024
4. Advisory issued from FIU-IND, Department of Finance ,Ministry of Finance, Govt. of India dated 26.10.2023 on Advisory for discouraging the opening and operations of Mule Account to prevent Cyber Enabled Frauds- reg:-
5. Advisory issued from RBI, Department of Supervision , KYC AML Group , Central Office, Mumbai dated August 10,2022 on Frauds/Cybercrimes through investment /part time job/ponzi scheme scams.

The above revised Policy Document was duly approved by the Board of Directors in their meeting dated 30.03.2024 is enclosed.

Branches / Offices are advised to be guided by the contents of the said Policy Document and ensure strict compliance of the instructions contained therein.

(Saroj Ranjan Nayak)
General Manager
Operation & Services Department

यूको बैंक / UCO BANK
के वाई सी एवं ए एम एल सेक्ष
KYC & AML Cell
प्रधान कार्यालय, कोलकाता / Head Office, Kolkata

Encl : As above.

Modifications/Additions in the existing Policy Document on KYC norms/AML standards/CFT/Obligation of Banks under PMLA, 2002 up to 31.01.2024 for FY 2024-25

Review of policy Document on KYC & AML

Page No	Existing Policy	New Page No.	Proposed Policy
Page no. 3	**3. <u>Definition of a customer</u>** A person or an entity that maintains an account and / or has a business relationship with the Bank;	**Page no.3 (Modification)**	**3. <u>Definition of a customer</u>** "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. as per the RBI/DBR/2015-16/18 Master Direction DBR.AML.BC No. 81/14.01.001/2015-16 dated 25.02.2016 updated as on January 04, 2024
Page No 29	**5.2.4.2iv) Accounts of Politically Exposed Persons (PEPs)** Politically exposed persons are individuals who are or have been entrusted with prominent public functions ~~in a foreign country~~, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials	**Page No. 29** (Modification)	**5.2.4.2 iv) Accounts of Politically Exposed Persons (PEPs)** Politically exposed persons are individuals who are or have been entrusted with prominent public functions **by a foreign country,** including the Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials as per the RBI/DBR/2015-16/18 Master Direction DBR.AML.BC No. 81/14.01.001/2015-16 dated 25.02.2016 updated as on January 04, 2024
Page no. 30	**5.3 Monitoring of Transactions** Accounts classified under High Risk category should be subjected to more frequent or ~~intensive~~ monitoring taking into account the customer's background, such as country of origin, source of funds, client's business and location, the type of transactions involved and other	**Page no.30 (Modification)**	**5.3 Monitoring of Transactions** Accounts classified under High Risk category should be subjected to more frequent or **intensified** monitoring taking into account the customer's background, such as country of origin, source of funds, client's business and location, the type of transactions involved and other risk factors.

	risk factors.		as per the RBI/DBR/2015-16/18 Master Direction DBR.AML.BC No. 81/14.01.001/2015-16 dated 25.02.2016 updated as on January 04, 2024
Page no. 34	**5.3.2 Operation of Bank accounts and Money Mules:**	*Page no. 34 (Addition)*	**5.3.2 Operation of Bank accounts and Money Mules:** **<u>FIU-INDIA Advisory</u>** In this regard, the FIU-IND has issued a detailed advisory dated 26.10.2023 for discouraging in opening and operations of Mule Account to prevent Cyber Enabled Frauds. FIU-India has given all its recommendations under six categories. **1:** Establishment of common standard to detect and discourage Mule Accounts. **2:** Sharing information across financial institutions to mitigate the migration of actors behind mule account to other bank/ institutions. **3:** Implementation of Behavioural Biometrics to enhance the detection capabilities. **4:** Mechanism to assign Risk score to the accounts. **5:** Restricting fund flow/final withdrawal in such accounts whenever suspicious activity alert is flagged on the basis of the RFIs related to Mule Account, **6:** Framework on Network Linkages of accounts through which cyber Fraud happened to trail the money to catch hold the person behind this and to return the money back to victim. **<u>Role of Branches while Opening of Account</u>** While opening account, Branches to scan profile of the customer. Following points to be considered:- a) Business/Occupation b) Permanent Address/Present Address c) Annual Income (e.g. Home-

			maker: Annual Receipts from spouse and for students-Annual receipts from parents to be considered). d) Customers having very low income should be monitored for having multiple accounts. e) Date of Birth f) Customer Risk Categorisation g) Verification of OVDs (in addition to verifying from original; OVDs should also be checked by downloading and searching the CERSAI portal). h) Biometric E-KYC of Aadhaar enabled customers. i) Customer behaviour in accordance to the profile of customer. j) Mobile number of the customer. k) In the account opening form, branch should that residential address columns is complete . If address in Aadhaar contains less details, alternate address proof or declaration should be insisted so that the address provided can be traced if need arises. l) Permanent Address and Present Address should be supported with authentic documents as per KYC norms. m) CKYC ID to be allotted immediately while opening of account. n) E-KYC to be done wherever accounts are opened through Aadhaar to enhance the ac-

			curacy and security of identity verification. o) Junk value/data or imaginary information should be avoided. p) Accounts opened by BCs should be checked meticulously by the branches. For implementation of advisory of FIU-IND on detection of mule accounts and transaction monitoring on real-time at central level is under progress and subject to a machine learning and AI based technology available at peer banks/market and further consulting with FIU-IND. As per the advisory issued by FIU-IND dated 26.10.2023.
Page no. 36	**5.3.2 Operation of Bank accounts and Money Mules:** **Monitoring through Red Flagging in Finacle System**	*Page no. 36 (Addition)*	**5.3.2 Operation of Bank accounts and Money Mules:** **As per RBI Advisory** Suspected money mule accounts will be reflected as red flagged in Finacle system to branches for which branches may be enabled to convert the flag 'Yes/No' within turnaround time(TAT) after completion of EDD. Mule Account detected by branches will be restricted for debit transaction while turning the red flagged 'Yes'. as per the advisory issued by RBI dated 10.08.2022
Page no 50	**5.4.5 <u>Periodic Updation of KYC</u>**	**Page no. 50 (Addition)**	**5.4.5 <u>Periodic Updation of KYC</u>** **4) <u>Partial freezing of transactions in non complied customers due for REKYC</u>** **a) First Notice**- Prior to 90 days of due date of RE-KYC, 30 days notice will be made available to branch in Finacle System. Branch will dispatch the notice

			to customer within 07 days by registered post/speed post or authentic courier service and the ID number issued by Post Office/Courier Service should be seeded in Finacle system by branch otherwise day end of branch will be restricted automatically by the Central Server. **b) Second Notice**- Prior to 60 days of due date of RE-KYC, 30 days notice will be made available to branch in Finacle system. Branch will dispatch the notice to customer within 07 days by registered post/speed post or authentic courier service and the ID number issued by Post Office/Courier Service should be seeded in Finacle system by branch otherwise day end of branch will be restricted automatically by the Central Server. **c) Third or Final Notice-** Prior to 30 days of due date of RE-KYC, 30 days notice will be made available to branch in Finacle system. Branch will dispatch the notice to customer within 07 days by registered post/speed post or authentic courier service and the ID number issued by Post Office/Courier Service should be seeded in Finacle system by branch otherwise day end of branch will be restricted automatically by the Central Server. After sending the final notice to customer, account will be frozen for debit transaction on due date of RE-KYC or expiring date of notice

			whichever is later. **RE-KYC process should be started prior to 180 days from the due date.**
Page no 56	**15. Freezing of Assets under sec 51A of Unlawful Activities (Prevention) Act 1967** **(i) Requirements/obligations under International Agreements Communications from International Agencies –** (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/ohz5jen-al-qaida.html**~~ (b) The " Taliban 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/3app1en-taliban.htm**~~	**Page no. 56** (Modification)	**15. Freezing of Assets under sec 51A of Unlawful Activities (Prevention) Act 1967** **(i) Requirements/obligations under International Agreements Communications from International Agencies –** (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 **www.un.org/securitycouncil/sanctions/1267/aq sanctions list** (b) The " Taliban Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at **https://www.un.org/securitycouncil/sanctions/1988/materials** as per the RBI/2023-24/111 DOR.AML.REC.69/14.06.001/2023-24 dated January 11,2024
Page No. 84	**38.Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):**	**Page No.84 (Addition)**	**38.Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):** The latest version of the UNSC Sanctions lists on DPRK is accessible on the UN Security Council's website at the following URLs: **https://www.un.org/securitycouncil/s**

UCO BANK KYC & AML Cell Head Office, Kolkata

			anctions/1718/materials as per the RBI/2023-24/109 DOR.AML.REC.67/14.06.001/2023-24 dated January 06,2024

यूको बैंक UCO BANK
सम्मान आपके विश्वास का HONOURS YOUR TRUST
(Government of India Undertaking)

POLICY GUIDELINES
ON
KNOW YOUR CUSTOMER (KYC) NORMS/ ANTI-MONEY LAUNDERING (AML) STANDARDS/ COMBATING OF FINANCING OF TERRORISM (CFT)/ OBLIGATION OF BANKS UNDER PMLA, 2002 ,
FY-2024-25

केवाईसी एंड एएमएल सेल, प्रधान कार्यालय –१, १ तल, भारतीय विपणन स्थान, कोलकाता,७००००१
KYC & AML Cell, Head Office-I, 1ST FLOOR. INDIA EXCHANGE PLACE, KOLKATA - 700 001
Ph No.: 03344557190 Fax: 03344559405/9425 Email: ho.kycaml@ucobank.co.in
राजभाषा का प्रकाश–बैंक का विकास

INDEX

LIST OF ANNEXURES

KYC/AML/CFT POLICY

POLICY GUIDELINES ONKNOW YOUR CUSTOMER (KYC) NORMS/ ANTI-MONEY LAUNDERING (AML) STANDARDS/COMBATING OF FINANCING OF TERRORISM (CFT)/OBLIGATION OF BANKS UNDER PMLA, 2002 AS AMENDED UPTO 04.01.2024 for FY 2024-25

1. PREAMBLE

On the recommendations of the United Nations, the Government of India has enacted Prevention of Money Laundering Act (PMLA) 2002 which has undergone certain amendments from time to time. It forms the core of the legal framework put in place by Government of India to combat money laundering. PMLA and the Rules notified there under impose an obligation on banking companies, Financial Institutions, Intermediaries of the securities market (i) to verify identity of client, (ii) to maintain records, and, (iii) to furnish information to the Financial Intelligence Unit-India (FIU-IND), which has been established as the Central Nodal Agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes. Director (FIU-IND) and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections to implement the provisions of the Act.

Money laundering is the process whereby proceeds of crimes, such as, drug trafficking, smuggling, etc. are converted into legitimate money through a series of financial transactions making it quite difficult to trace back the origin of funds. Further, the technological advancements have helped money launderers to adopt innovative means and move funds faster across continents making detection and preventive action much more difficult. This calls for a sensitized approach in tracking the crime on the part of the Banks who need to be more vigilant and prudent in undertaking Due Diligence while opening accounts and also to monitor closely the operations in the accounts.

Bank has been following customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. Our "Know Your Customer" 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), Foreign Accounts Tax Compliance Act (FATCA) and in the light of the subsequent changes in the regulatory guidelines. India has been admitted as a member country in FATF in June 2010 and the current membership is 39. FATF came with 40 recommendations along with 9 special recommendations as a measure to combat terrorist financing and include measures to be taken by countries to criminalize terrorist financing, ratification and implementation of UN resolutions on terrorism, freezing and confiscation of terrorist assets etc.

This policy document is an update on revisited guidelines/instructions received from Reserve Bank of India in the context of recommendations of FATF on Anti Money Laundering (AML) standards, combating Financing of Terrorism (CFT),

Customer Due Diligence (CDD) for Banks and also in the context of amendments in Prevention of Money Laundering Act 2002.

2. OBJECTIVE AND SCOPE

The Policy has been framed to develop a strong mechanism for achieving the objective of preventing misuse of banking channel for illegal purposes and ascertaining the genuineness of customers and keeping a track of operations to trace out any suspicious transaction/activity in conduct of customers' operations including the system of purchase and/or sale of foreign currency notes/Travellers' Cheques by Banks/ Authorized Persons from being used, intentionally or unintentionally by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable Banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

The offence of Money Laundering has been defined in Section-3 of the Prevention of Money Laundering Act, 2002 as "whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money laundering". Money Laundering can be called a process by which money or other assets obtained as proceeds of crime are exchanged for "clean money" or other assets with no obvious link to their criminal origins. It involves creating a web of financial transactions so as to hide the origin and true nature of these funds.Sec.12 casts statutory obligation on every banking company, financial institution, intermediaries and other prescribed reporting entities, and failure to comply with these obligations may attract imposition of (as per Sec.13 of PMLA of 2002) levy of fine not less than Rupees Ten Thousand extendable to Rupees one lac for each failure.

In terms of PML Rules, groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002. (15 of 2003). Accordingly, every bank-branches which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

For the purpose of this document, the term money laundering would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

This policy is applicable to the Bank's Branches located in India or Abroad, to the extent they are not contradictory to the local laws in the Host country, provided that**:**

(i) Where local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of KYC & AML Cell, HO. RBI may advise further necessary action by the banks including

application of additional measures to be taken by the branches to manage the ML/TF risks.

(ii) In case there is variance in KYC/AML standards prescribed by Bank and Host country regulators, Branch/overseas subsidiaries of Bank are required to adopt more stringent of the two.

3. Customer

A customer for the purpose of this policy is defined as:

- "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.

"Aadhaar Number "

- "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);

- One on whose behalf the account is maintained (i.e. the beneficial owner);(Ref: GOI Notification dated 12.02.2010-Rule 9,Sub rule(1A) of PMLA Rules 'beneficial owner means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person')

- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc. as permitted under the law; and

- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank, say any Wire transfer or issue of high value demand draft on a single transaction.

4. Definition of Transaction:

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

(a) Opening of an account;
(b) 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;
(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 of any contractual or other legal obligation;
(f) Establishing or creating a legal person or legal arrangement.

5. ELEMENTS of KYC POLICY

KYC policy has been framed incorporating the following four key elements:

- Customer Acceptance Policy (CAP)
- Customer Identification Procedures (CIP)

- ✓ Video Customer Identification Procedure (V-CIP)

- Monitoring of Transactions
- Risk Management

5.1 CUSTOMER ACCEPTANCE POLICY (CAP)

Branches will accept customers after verifying their identity as laid down in customer identification procedures and exercising checks to ensure that the identity of the customer does not match with any other person with known criminal background or with banned entities. Customer Acceptance Policy lays down explicit guidelines on the following aspects of customer relationship in the bank.

- Not to open account in the name of anonymous / fictitious / benami name(s). [Branches will not allow the opening of or keep any anonymous account or accounts in fictitious name or account on behalf of other persons whose identity have not been disclosed or cannot be verified].

- Not to accept customers where the Branch is unable to apply appropriate customer Due Diligence measures i.e. Bank is unable to verify the identity and or obtain documents required as per the risk categorization either due to non-cooperation of the customer or non-reliability of the data / information furnished to the Bank.**The bank shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.** It is, however, necessary to ensure that no harassment is caused to the customers, particularly to the small deposit customers. Decision by the Branch in regard to closure of an account should be taken at higher level after giving due notice to the customer explaining the reason for such a decision.

- While accepting customers**,** the Branches should ensure that all documentation requirements and other information in respect of different categories of customers depending on perceived risk have to be collected, which should result in preparing a profile for each new customer. The details of documentation to be obtained for each category of customers are to be as per the Bank's Deposit Manual of Instructions. The broad features to be verified and documents to be obtained from the customers are spelt out in brief in **Annex-1.**

- 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 as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

- Necessary checks should be made before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. as circulated by Head Office on the basis of RBI Notification, also accessible on the UN website: http://www.un.org/sc/committees/1267/. The list is also accessible on Bank's intranet IRPS (KYC/AML) portal as well as in FINACLE (CBS) System.

- The customer profile would contain information relating to customer's identity, social/financial status, nature of business activity, information about

his clients' business and their location etc. The nature and extent of Due Diligence will depend on the risk perceived. Care to be taken to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

- Mandatory information required for KYC purpose (which is mentioned in various HO circulars and policy documents on KYC/AML) which the customer is obliged to give while opening an account only should be obtained at the time of opening the account/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.

- Branches should verify the identity of the Politically Exposed Persons (PEP) and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP should be taken by the Branch Head. Details of Identification of PEP are spelt out in subsequent paragraphs.

- Those persons who do not have Aadhaar/Enrolment number and PAN and desire to open Bank account can open 'small accounts' on the basis of a self-attested photograph and putting his/her signature or thumb print in the presence of an official of the Bank. Details are given in the subsequent paragraphs under 'small accounts'.

- Branch should obtain "No Objection Certificate" from the lending bank before opening current account of a customer who has availed any loan/advance/cc limits earlier.

- It is important to bear in mind that the adoption of Customer Acceptance Policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those who are financially and socially disadvantaged.

5.2 Customer Identification Procedure:

Customer identification means identifying the customer and verifying his / her identity by using reliable, independent source documents, data or information. Branches need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship as mentioned/specified in Account Opening Form. Being satisfied means 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.

- The Customer Identification Procedure will be carried out:

  i. At the time of commencement of an account based relationship with the customer.

  ii. Carrying out any international money transfer operations for a person who is not an account holder of the Bank.

iii. When there is a doubt about authenticity or adequacy of the identification data already obtained by the Bank.

iv. Selling third party product as agents, selling bank's own products, payment of dues of credit card/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

v. When the Bank feels it is necessary to obtain additional information from the existing customers based on the conduct/ behaviour of the account.

vi. 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 rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

vii. However, if Branch has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rupees fifty thousand only.

viii. Banks shall ensure that introduction is not to be sought while opening accounts.

- For the purpose of verifying the identity of customers at the time of Commencement of an account-based relationship, Banks may rely on customer due diligence done by a third party, subject to the following conditions:

i. 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.

ii. Adequate steps are taken by Banks 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.

iii. 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.

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

v. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Bank.

5.2.1 Video Customer Identification Procedure(V-CIP):-

Branches may undertake V-CIP to carry out:

(i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

(ii)Provided that in case of a proprietorship firm, branches shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in section 5.2.3.2, apart from undertaking CDD of the proprietor.

(iii)Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 5.2.3.16.2

(iv) Updation/Periodic updation of KYC for eligible customers.

Bank/Branches opting to undertake V-CIP shall adhere to the following minimum standards:

(a) V-CIP Infrastructure

(i) The Bank should have to comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the bank and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

(ii) The bank/branch shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

(iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the bank/branch. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

(vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber-security event under extant regulatory guidelines.

(vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, and maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

(i) Bank shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the bank/branch specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

(ii) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

(iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

(iv) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

(v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

(vi) The authorised official of the bank/branch performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

(a) OTP based Aadhaar e-KYC authentication
(b) Offline Verification of Aadhaar for identification
(c) KYC records downloaded from CKYCR, in accordance with section 9 of this policy, using the KYC identifier provided by the customer
(d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi-Locker.

Bank/branch shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

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 working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, bank/branch shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, bank/branch shall ensure that no incremental risk is added due to this.

(vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

(viii) Bank/branch 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 including through Digi Locker.

(ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

(x) The authorised official of the bank/branch shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

(xi) Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. 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.

(xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

(xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Bank.

(c) V-CIP Records and Data Management

(i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this policy, shall also be applicable for V-CIP.

(ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

5.2.2 Customer Due Diligence (CDD)-General Guidelines

- Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial ownerusing reliable and independent sources of identification.

  Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
(c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

- Branches to apply CDD procedure at the UCIC level. If an existing KYC Compliant customer desires to open another account with our Bank, there shall be no need for a fresh CDD exercise.
- Branches to undertake client Due Diligence measures while commencing an account-based relationship. Such measures include identifying and verifying the customer and beneficial owner, their location and financial status on the basis of reliable and independent information and data or documentation.
- Apply client Due Diligence measures to existing clients at an interval of two/eight/ten years in respect of high/medium/low risk clients respectively.
- Carry out ongoing Due Diligence of existing clients in order to ensure that their transactions are consistent with the bank's knowledge of the client, his business and risk profile and where necessary, the source of funds.
- Branches need not seek fresh proof of identity and address at the time of periodic Updation, from those customers who are categorized as 'low risk', in case there is no change in status with respect to their identity and address. 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 may not insist on physical presence of such low risk customer at the time of periodic Updation. For all other customers, an Officially Valid Document to be submitted having current address.
- 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.
- For customers that are natural persons the Branch should obtain sufficient identification data to verify the identity of the customer, his address / location, and also his recent photograph.
- For customers that are legal persons or entities, the Branches should (i) verify the legal status of the legal person or entity through proper and relevant documents; (ii) Verify that the person purporting to act on behalf of the legal person / entity so authorized and identify and verify the identity of that person; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person/entity.
- Whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact,

pose a low risk, Branches should carry out full scale customer Due Diligence (CDD) of the customer.

- When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, Branches should review the Due Diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship.

- Branches are advised that KYC once done by one Branch of the bank should be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account. The customer should be allowed to transfer his account from one Branch to another Branch without restrictions. Branches may 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

- Branches should ensure that periodical Updation of customer identification data (including photograph/s) to be up to date after the account is opened. The periodicity of such Updation should not be less than once in ten years in case of low-risk category customers, eight years in medium risk category and two years in case of high-risk categories. Fresh CDD &photographs are required to be obtained from minor customer on becoming major.

- In the circumstances when Branches believe that it would no longer be satisfied about the true identity of the account holder, it should also file an STR with FIU-IND.

- Branches have been allowed to carry out Aadhaar authentication/offline-verification of an individual who voluntarily uses his Aadhaar number for identification purpose.
- Proof of possession of Aadhaar number has been added to the list of Official Valid Documents (OVD) with a proviso that where a customer submits "Proof of possession of Aadhaar" as OVD, he/she may submit it in such form as are issued by Unique Identification Authority of India (UIDAI).

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

- **For existing customers of the Bank, PAN/Form No-60 is to be submitted within such timelines as may be notified by the Government, failing which the account shall be subject to temporary ceasing till PAN/Form No.60 is submitted. However, before temporarily ceasing operations for an account, the customer is to be given an accessible notice period not more than 30 days and a reasonable opportunity to be heard.**
  For customers who are unable to provide PAN or Form No. 60 owing to injury, illness, infirmity on account of old age or out of station, Branch Head may take decision to further extension of notice period up to3 months. However, Branch will consider such accounts for enhanced monitoring of transactions.
- **In terms of provisions of Rule 114B of Income Tax Rules, Quoting of PAN number is mandatory while opening an account or making a time deposit 50000 and above and any individual who does not have PAN shall make a declaration in Form 60 for the transaction [Bank Circular**

no.CHO/SUA/08/2016-17 dated 21.06.2016. PAN is compulsory for opening of accounts except BSBD & small accounts.

- Branch shall obtain the Aadhaar number from an individual who desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act. Branch at receipt of the Aadhaar number using e-KYC authentication facility provided by the UIDAI on receipt of customer declaration that he/she desirous of receiving any benefit or subsidy under any Scheme notified under section 7 of the Aadhaar Act.

- Branch may carry out Aadhaar authentication/ Offline verification of an Individual customer who voluntarily uses his Aadhaar number for identification purpose.

- Where an equivalent e-document is obtained from the customer, Bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- In case the customer is not a resident or resident in states of Jammu &Kashmir, Assam and Meghalaya and does not submit the PAN, the customer shall submit a certified copy of officially valid documents containing details of his identity and address, one recent photograph and such other document including in respect of the nature of business and financial status as may be required by Bank.

5.2.3 Customer Due Diligence - Procedure

5.2.3.1 Individual Customers:

Branches to obtain the following documents 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:

i. (a) the Aadhaar number where,
He/she 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
He/she decides to submit his/her Aadhaar number voluntarily to the bank; 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;

(ac) the KYC identifier with an explicit consent to download records from CKYCR.

ii. PAN or Form-60 as defined in Income Tax rules, 1962 as amended from time to time.

iii. One recent Photograph

iv. A Original certified copy of any OVD containing details of identity & address

v. Such other documents pertaining to the nature of business or financial status as decided by the branch. Few such documents are listed hereunder:

- Utility bill which is not more than two months old of any service provider (Electricity, Telephone, Postpaid Mobile phone, Piped gas, Water bill)
- Property or Municipal tax receipt
- Pension or family pension payment order(PPOs) issued to retired employees by Government Departments or Public Sector undertakings, if they contain the address
- Letter of allotment of Accommodation from employer issued by Central Govt. departments, Statutory Regulatory Bodies, PSUs, SCBs, FIs & listed companies. Similarly Leave &License agreements with such employers allotting official accommodation.

Provided that where the customer has submitted,

i) Aadhaar number under clause (a); bank 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 Bank.

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

iii) An equivalent e-document of any OVD, the Branch 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(A).

Provided that for a period not beyond such date as may be notified by the Government for a class of Bank, instead of carrying out digital KYC, the Bank 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.

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

v) KYC identifier under clause (ac) above, the Banks shall retrieve the KYC records online from the CKYCR in accordance with section 56.

i) Bank shall obtain the Aadhaar number from an individual who desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act. Bank at receipt of the Aadhaar number using e-KYC authentication facility provided by the UIDAI on receipt of customer declaration that he/she desirous of receiving any

benefit or subsidy under any Scheme notified under section 7 of the Aadhaar Act.

ii) Branch may carry out Aadhaar authentication/ Offline verification of an Individual customer who voluntarily uses his Aadhaar number for identification purpose.

a. "Authentication", in the context of Aadhaar authentication, means the process as defined under sub section (c) of section 2 of Aadhaar (Targeted delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

b. Certified Copy" - Obtaining a certified copy by the Bank 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 Branch as per the provisions contained in the Act.

c. "Offline Verification", as defined in the Aadhaar and other Law (Amendment) Ordinance, 2019, means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

iii) For other Non DBT beneficiary customers, the Bank shall obtain a certified copy of OVD containing details of his identity and address along with one recent photograph.

iv) Branches should ensure that the Non DBT beneficiary customers, while submitting Aadhaar for Customer Due Diligence (CDD) redacts or blackout their Aadhaar number in terms of sub-rule 18 of Rule 9 of the amended PML Rules.

v) "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 Branch as per the provisions contained in the Act **(Annexure 1(A)**).

vi) "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).

vii) "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.

viii) "**Video based Customer Identification Process (V-CIP)"**: An alternate method of customer identification with facial recognition and customer due diligence by an authorised official by an official of the Bank 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 through independent verification and maintaining audit trail of the process . Such process complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this policy.

In cases where successful authentication has been carried out, other OVD and photograph need not be submitted by the customer.

Provided further that in case biometric 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, Bank 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 from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank/Branch and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. Bank has 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 Bank and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

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, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

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

In case the OVD furnished by the customer does not contain 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, Postpaid Mobile phone, Piped gas, Water bill)

ii) Property or Municipal tax receipt

iii) Pension or family pension payment order(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 Central Govt. departments, Statutory Regulatory Bodies, PSUs, SCBs, FIs & listed companies. Similarly Leave & License agreements with such employers allotting official accommodation.

The customer should submit OVD updated with current address within a period of three months of submitting the above documents**.**

In case an individual customer who does not possess any of the OVDs and desires to open a bank account, branch shall open a 'Small Account'. Details of Small Account are narrated in Point No. 5.2.3.15.

CDD in Joint Accounts: While opening Joint accounts (Either/survivor, Former/Survivor, Jointly, Later/Survivor etc.). Customer due diligence procedure to be carried out in the same way as that of Individual customers for every joint holder.

5.2.3.2 Accounts of proprietary concerns

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

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, Branches should call for and verify the following documents before opening of accounts in the name of a proprietary concern: Proof of the name, address and activity of the concern, like

1. Registration certificate (in the case of a registered concern) including Udyam Registration Certificate (URC) issued by the Government.
2. certificate/licence issued by the Municipal authorities under Shop & Establishment Act,
3. sales and income tax returns, CST/VAT/GST certificate(Provisional/Final), certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities,
4. Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities,
5. Registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department.

Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, 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 and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

Apart from the identity & address of the proprietor, any two of the above documents or equivalent e-document would suffice. These documents should be in the name of the proprietary concern.

In cases where the Bank is satisfied that it is not possible to furnish two such documents, Bank may, at their discretion, accept only one of those documents as proof of business/activity. However, Zonal Manager will be the competent authority to decide such waiver.

5.2.3.3 Walk-in Customers

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 rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. However, if Branch has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50, 000/- it would verify the identity and address of the customer and also consider filing a suspicious transaction report (STR).

Customer identification procedure is to be carried out in respect of non-account holders (walk-in-customers) approaching bank for high value one-off transaction or several transactions that appear to be connected.

5.2.3.4 Trust/Nominee or fiduciary Accounts:

Branches should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, Branches should insist on receipt of 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. While opening an account for a trust, Branches should take reasonable precautions to verify the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

5.2.3.5 Account of Companies:

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the Bank. Branches 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.

Documents required for opening an account of Company are specified in **Annex-1**.

5.2.3.6 Client Accounts opened by Professional Intermediaries:

When Branches have 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. Branches may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Pooled accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients are also maintained at Branches. Where funds held by the intermediaries are not co-mingled 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, the Branches should still look through to the beneficial owners. Where "customer Due Diligence" (CDD) is done by an intermediary, Branches should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the Branches of the bank.

Under the extant AML/CFT framework, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. It is reiterated that Branches should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits bank's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, would not be allowed to open an account on behalf of a client.

5.2.3.7 Accounts of non-face-to-face customers

Introduction of telephone and electronic communication is playing a vital role in day-to-day banking. At times, requests are received telephonically or electronically to open accounts of those persons who are stationed at centers other than the Branch locations. This is a case where the Branches are required to open the accounts of non-face-to-face customers, i.e. of the customers with whom the Branch officials have not had direct interaction (with the prime holder of individual account or one of the signatories of non-individual / joint account) at the time of opening the account. Branches 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 additional difficulty of matching the customer with the documentation and the Branch 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 System in place.

5.2.3.8 Procedure to be followed in respect of foreign students.

Branches should follow the following procedure for foreign students studying in India.

- Branches may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.

- Within a period of 30 days of opening the account, the foreign student should submit to the Branch where the account is opened, a valid address proof giving local address, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility provided by the educational institution. Branches should not insist on the landlord visiting the Branch for verification of rent documents and alternative means of verification of local address may be adopted by banks.

- During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs.50,000/-, pending verification of address.

- On submission of the proof of current address, 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.

- Students with Pakistani nationality will need prior approval of the Reserve Bank for opening the account.

5.2.3.9 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) Customer Due Diligence(CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

5.2.3.10 Prepaid payment Instruments :

Prepaid payment instruments are payment instruments that facilitate purchase of goods and services against the value stored on such instruments. The value stored on such instruments represents the value paid for by the holder, by cash, by debit to a bank account, or by credit card. The instruments can be issued in the country. The use of such instruments for cross-border transactions shall not be permitted except for the payment instrument issued by authorized person under the FEMA guidelines. The maximum value of any prepaid payment instruments shall not exceed Rs.50, 000/-.

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

The name of purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque etc by the issuing bank.

Cheques/drafts/pay orders/banker's cheques bearing the date or any subsequent date, if presented beyond the period of three months from the date of such instrument, would not be paid. Provisions of Foreign Contribution (Regulation) Act, 2010, wherever applicable, are to be strictly adhered to.

5.2.3.11 Sale of Third Party Products :

While selling third party products as agents, (a) Branches should verify the identity and address of the walk-in customer. (b) Branches should also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed under PML rules. (c) The instructions to make payment by debit to customers' accounts or against cheques for remittance of funds/issue of travelers' cheques, and the requirement of quoting PAN number for transactions of Rs.50,000 and above, would also be applicable for to sale of third party products by the bank as agents to customers, including walk-in customers.

The instructions in respect of third party products would also apply for selling of banks' own products, above Rs.50,000/-.

Branches would verify the PAN numbers given by the account holder as well as walk-in customers so that dummy/fictitious PAN numbers are not quoted for transactions of Rs.50, 000/- and above.

Banks' AML software would be enabled to capture, generate and analyze alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers, sale of third party products, and transactions involving internal accounts. The utility of the CTR/STR alerts for risk categorization of customers would also be examined.

5.2.3.12 Foreign Portfolio Investors (FPIs)

In terms of Rule 9 (14)(i) of 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 Branch for opening a Bank Account for the purpose of investment under Portfolio Investment Scheme (PIS). Details of KYC requirement for eligible FPIs are given in Annex-14 subject to Income Tax (FATCA/CRS) Rules.

5.2.3.13 Accounts of Juridical persons etc.:

For opening of accounts juridical persons such as govt. or its departments, societies, universities, and local bodies like village panchayat etc., a certified copy of the following documents to be obtained:

i. Document showing name of the person authorized to act on behalf of the entity.

ii. Officially valid documents(OVDs) for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf

iii. Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person (DBR.AML.BC.No.18/14/.01.001/2016-17 dated 08.12.2016)

5.2.3.14 Small Accounts- Reduced KYC procedure

A 'Small Account' means a savings account where:

- The aggregate of all credits in a financial year does not exceed Rs.100000/-
- The aggregate of all withdrawals and transfers in a month does not exceed Rs.10000/- and
- The balance at any point of time does not exceed Rs.50000/.Provided, that, this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Opening of a Small Account

A 'small account' may be 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:

The designated officer of the Branch while opening the small account certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;

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.

- A small account shall be opened at Branches. The account to be monitored manually so as to ensure that foreign remittance is not credited to the account and that the aggregate stipulated limit of monthly and annual transactions and balance in such accounts are not breached, before a transaction is allowed to take place;
- 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 to the Branch for having applied for any of the officially valid documents within twelve months of opening of the said account. The entire relaxation provision to be reviewed in respect of the said account after twenty four months.
- A small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios,

the identity of customer shall be established through the production of "officially valid documents"; and

- 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".
- 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.

The customers having small accounts to be made aware that if, at any point of time, the balances in all his / her accounts with the Bank taken together exceed Rs.50,000/- or total credit in all the accounts exceeds Rs.1 lakh, no further transaction will be permitted until full KYC procedure is completed. An undertaking (as per the specimen available at **Annex-3)** to this effect be obtained from the customer at the time of opening the account itself. The amount of one-time payments from government or other agencies on exceptional circumstances (death claims, grant of relief, etc.) be excluded from the threshold limit of Rs.50, 000/- or Rs.1, 00,000/-, as the case may be. In order to avoid any inconvenience to the customers, the Branches should notify to the customer (as per the specimen available at Annex-4) when the balances reach Rs.40,000/- or the total credit in a year reaches Rs.80,000/- that appropriate documents for complying the KYC must be submitted otherwise operations in the account should be stopped.

5.2.3.15 Basic Savings Bank Deposit (BSBD) Account

5.2.3.15.1 The "Basic Savings Bank Deposit Account" shall offer following minimum common facilities to all the customers:

a) The Basic Savings Bank Deposit Account shall be considered a normal banking service available to all.

b) This account shall not have the requirement of any minimum balance.

c) The services available in the account will include deposit and withdrawal of cash at bank Branch as well as ATMs; receipt/credit of money through electronic payment channels or by means of deposit/ collection of cheques drawn by Central/ State Government agencies and departments.

d) While there will be no limit on the number of deposits that can be made in a month, account holders will be allowed a maximum 10 number of withdrawals will be allowed in a month with a cap of 4 withdrawals through ATM & with cap of 6 cash withdrawals at branch and BC point.

e) A cheque book allowed to the fully KYC complied account.

f) Facility of ATM card or ATM-cum-Debit Card.

The above facilities will be provided without any charges. Further, no charge will be levied for non-operation/ activation of inoperative Basic Savings Bank Deposit Account. Additional value added services beyond the stipulated basic minimum services will be chargeable.

The Basic Savings Bank deposit Account would be subject to RBI instructions on Know Your Customer (KYC)/ Anti-Money laundering (AML) for opening of bank accounts issued from time to time.
If such account is opened on the basis of simplified KYC norms, the account would additionally be treated as a "Small Account" and would be subject to conditions stipulated for such accounts as detailed under para 6.03.2.1.

Holders of Basic Savings Bank Deposit Account will not be eligible for opening any other savings bank deposit account in the Bank. If a customer has any other existing savings bank deposit account in the Bank, he/she will be required to close it. The existing basic banking "no frills" accounts which was introduced in 2006 will be treated as Basic Savings Bank Deposit account.

5.2.3.15.2 Accounts opened using OTP based e-KYC, are subject to the following conditions:

- There must be a specific consent from the customer for authentication through OTP.
- As a risk mitigating measure for such accounts, Banks/branches should ensure that transaction alerts, OTP, etc. are sent only to the mobile number of the customer registered with Aadhaar. For dealing with request received for change in mobile no. , branch should follow proper procedure for verification of new mobile no. by OTP based e-KYC as such mobile number available /updated with UIDAI only.
- 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 is completed.
- The aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed rupees two lakh.
- 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.
- Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which Customer Due Diligence (CDD) procedure or (V-CIP) is to be completed. If the CDD procedure 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.
- 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 either with the bank/branch or with any other bank. Further, while uploading KYC information to CKYCR, branches shall clearly indicate that such accounts

are opened using OTP based e-KYC and other banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure.

- Alerts to be generated in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

5.2.3.16 Beneficial owners

Based upon the risk profile of the customer, Branch should ensure to take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is known /established who the beneficial owner(s) is/are. Beneficial Owner is a "natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person". Procedure for determination of Beneficial Ownership shall be in line with the procedure as advised by Government of India **[Annex -2].**

5.2.3.17 Application of KYC norms

- For the purpose of applying KYC norms, reasonable steps should be taken to verify the identity and reputation of any agent / representative / attorney who opens / operates account on behalf of the applicant.

- When signatories change, care should be taken to ensure that the identity of the new signatory has been verified and their cust-id to be created and entered in related party details in CBS.

- Existing current accounts will be subjected to revised KYC procedures as per the guidelines formulated by the Bank for such accounts, applying the norms of materiality and risk.

- Branches should ensure that banking facilities are not denied for genuine purposes merely for the reason that criminal charges have been leveled against them or they have undergone some form of punishment in the past.

- Send a welcome letter to the new customer.

5.2.3.18 Obtention of documents

- The Customer Profile Form-for New & Existing Customers is to be drawn as advised in revised Account Opening Forms vide Head Office Circular no. CHO/OSD/31/2016-17 dated 16.04.2016. Keeping in view the risk profile of the customer, all relevant information has to be obtained with regard to customer's identity, social/financial status and nature of business activity etc.
- The set of Officially Valid Documents (OVD), as stated in **Annex-1,** should normally suffice to establish both the identity and correct address of the applicant.

- Each customer should be allotted a specific customer Identification Number (Cust ID number) and the same ID should be used for opening subsequent accounts of the same customer.

5.2.3.19 Mis-spelt names in the ID proof documents

- Accounts should be opened in the same name and style that appears in the documents that are submitted by the applicants for the purpose of identification. For example, if the documents submitted by an individual depict the name as Ram Kumar Sharma, then the account should be opened in the same fashion and not as "R.K Sharma, or Ram K. Sharma, or R. Kumar Sharma".

- In case an applicant writes spellings of his name in the Account Opening Form (AOF) which are different from the spellings appearing in the document submitted by him / her for the purpose of identification, the said document can be accepted provided the document is a photo document and the photograph and the address on the document is the same as that mentioned in the AOF.

5.2.3.20 Introduction – practice of obtaining thereof

Introduction is not mandatory for opening of accounts – Before implementation of the system of document –based verification of identity, as laid down in PML Act/Rules, introduction from existing customer was considered necessary for opening of the account. Since introduction is not necessary for opening of accounts under PML Act and Rules or Reserve Bank's extant KYC instructions. Branches should not insist on introduction for opening of bank accounts [DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016].

5.2.3.21 Obtention of photographs

- In all new deposit accounts, two recent photographs of the applicant (also applicable to non-resident customers) should be obtained and pasted on the Customer Profile Form and specimen signature Card. It should be ensured that the photograph of the applicant and his/ her actual appearance should resemble.

- In all subsequent deposit accounts opened by the depositor, no fresh photograph is to be obtained. However, a reference of the existing account (wherein the photographs are available) is to be made in all the relative AOFs. The cost of the photographs shall be borne by the customers.

- Signature / thumb impression of the prospective customer should be obtained on his / her photographs in such a manner that the signature / thumb impression of the customer lies partly on AOF and partly on the photograph.

- Thereafter, the photographs of the prospective customer should be attested by the person responsible for opening the account under his / her full signature with an ink which sticks on the photographs.

- Banks, local bodies, government departments and public sector under-takings excluding quasi-government bodies are exempt from the above requirement.

5.2.3.22 Reliance on third party Due Diligence

- For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, Branches may rely on a third party subject to the conditions that-
    - Records or the information of the customer due diligence carried out by the third party is obtained **immediately** from the third party or from the Central KYC Records Registry.
    - The Branch 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;
    - The Branch is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with the client Due Diligence and record-keeping requirements in line with the requirements and obligations under the Act;
    - The third party is not based in a country or jurisdiction assessed as high risk; and
    - The Branch is ultimately responsible for client Due Diligence and undertake enhanced Due Diligence measures, as applicable.

5.2.3.23 Certification and copying identification documents:

- To guard against the dangers of postal intercept and fraud, prospective customers should not be asked to send originals of valuable personal identity documents, e.g., passport, identity card, driving licence, etc. by post. Rather, they should be asked to bring the same personally in the Branch for the purpose of verification.
- Only the original document may be used as evidence of identity; but a photocopy, or where necessary multiple copies, of the original may then be made to record / certify that identification checks have taken place.
- Certified copies of identification evidence should be dated, and signed and marked as verified from original by the authorized officials only.

5.2.3.24 Action to be taken in the event of non-submission of the required data subsequently

- In the event of non-submission of the required papers / information by the customers, the Branches should proceed in the following manner:
    - In case there are abnormal transactions in the newly opened account where identification process has not been completed and the customer neither submits the required documents nor gives satisfactory reply to the abnormal transactions, the Branches should consider filing suspicious transaction/activity alert to Head Office through IRPS-> KYC/AML->Suspicious Activity Entry. In no circumstances customer concerned be tipped off.

- In case the value of transactions in the newly opened / existing accounts is abnormally higher than the known profile of the customer, the Branches should consider filing suspicious transaction/activity alert to Head Office through IRPS.

- It should be noted that the decision to close an existing account should be taken at the level of Branch Manager.

- Detailed procedure for sending suspicious transaction/activity report has been outlined in the subsequent paras.

- No account other than TD up to Rs.50, 000/-should be opened by the Branches without PAN Card except Basic Savings Bank Deposit & small accounts. In case of non-availability of PAN, Form 60 as defined in Income tax rules, 1962 to be obtained.

5.2.3.25 SECRECY/CONFIDENTIALITY OF CUSTOMER'S ACCOUNT/ INFORMATION

- The information collected from the customer for the purpose of opening of account would be treated as confidential and details thereof would not to be divulged for cross selling or any other like purposes. It would be ensured that information sought from the customer is relevant to the perceived risk and is not intrusive. Any other information from the customer would be sought separately with his/her consent after opening the account.

- Branches should not disclose details / particulars of the customer's account to a third person or party without the express or implied consent from the customer save where disclosure of information is necessary under compulsion of law, or where there is a duty to public to disclose and where interest of the Bank requires such disclosure.

- Information obtained from a customer, for a purpose other than KYC/AML requirements, should be collected after explaining the objectives to him / her and taking his / her express approval for the specific uses to which such information could be put.

- While considering the requests for data/information from Government and other agencies, branches 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.

- 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.

5.2.4 Enhanced Due Diligence (EDD) procedure:

In case the bank requires additional information on the customer for concluding the suspicion or otherwise, it may conduct an enhanced due diligence through the Branch manager or any other bank official having knowledge of the customer. Based on such customer information, objective parameters, judgment of business group, and banker's prudence, Banks arrive at a conclusion whether the transaction is suspicious or not. Some of the objective parameters which can be used for enhanced due diligence could be:

a. Customer location
b. Financial status
c. Nature of business
d. Purpose of transaction

EDD to be carried out in respect of the following types of Customers:

5.2.4.1 Accounts of non-face-to-face Customers

Non-face-to-face on boarding facilitates the banks to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, Digi-Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by banks / branches for non-face-to-face customer –

a) In case, Bank has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote on boarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Branch shall take a robust process of due diligence for dealing with requests for change of registered mobile number.

c) Apart from obtaining the current address proof, bank branches shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) Banks shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

5.2.4.2 Accounts of Politically Exposed Persons (PEPs)

Politically exposed persons are individuals who are or have been entrusted with prominent public functions by a foreign country, including Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials.

(i) Branches to gather sufficient information including information about the sources of funds, accounts of family members and close relatives of the PEPs.

(ii) The identity of the person should be verified before accepting the PEP as customer

(iii) All the accounts of PEPs are to be subjected to enhanced monitoring on an ongoing basis

(iv) The approval to open an account for a PEP shall be obtained from the senior management. Branches and the Zonal Head/ Dy. Zonal Heads in respect of the other Branches within their zones. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

(v) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, approval to continue the business relationship to be taken by the Branch Head of AGM/DGM/GM headed Branches and the Zonal Head/ Dy. Zonal Heads in respect of the other Branches within their zones.

(vi) The CDD measures as applicable to PEPs including enhanced monitoring on an ongoing basis are also applicable to the above.

(vii) EDD is also applicable to accounts where a 'PEP' is the ultimate beneficial owner.

The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

5.2.4.3 Client Accounts opened by Professional Intermediaries:

Branches to ensure while opening client account through a professional intermediaries:

(i) Client must be identified when client account is opened by professional intermediary on behalf of a single client.

(ii) Branches may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

(iii) Branches should not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosures of the client details to the Branch.

(iv) All the beneficial owners should be identified where funds held by the intermediaries are not co-mingled at the Bank level and there are 'sub-accounts' each of them attributable to a beneficial owner, or where such funds are co-mingled at Bank level, the

beneficial owners to be identified at Bank level.

(v) Branch should rely on CDD done by an intermediary, which 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 Branches of the bank.

5.2.4.4 Risk categorisation downgraded during Risk Review:

In case Risk category is downgraded during Risk review done on quarterly basis i.e. Risk downgraded from Low Risk to High Risk, Low Risk to Medium Risk and Medium Risk to High Risk. EDD for such customers shall become due on the date the Risk category for the customer has been downgraded i.e. the risk review date, the moment risk downgraded from the existing risk. Movement of risk from High to low, High to Medium and Medium to Low is considered as risk upgradation and no EDD is required in such cases.

5.3 MONITORING OF TRANSACTIONS

- Ongoing monitoring is an essential element of effective KYC procedure. Branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity**.** Besides they should pay special attention to the following type of transactions:

    - Large & complex transactions including RTGS/NEFT/IMPS/SWIFT transactions.

    - Transactions of unusual patters, inconstant with the normal and expected activity of the customer ,which have no apparent economic rational or legitimate purpose

    - Transactions which exceed threshold limit(s) prescribed by the Bank for a particular category of accounts

    - High account turnover inconsistent with the size of the balance maintained

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

Branches should pay particular attention to the. The following type of transactions shall necessarily be monitored:

- Transactions that involve large amount of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the field functionaries. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being "washed**"** through the account.

- Accounts classified under High Risk category should be subjected to more frequent or intensified monitoring taking into account the customer's background**,** such as country of origin, source of funds**,** client's business and location, the type of transactions involved and other risk factors. High risk associated with accounts of bullion dealers (including sub-dealers) &

jewelers should be taken into account to identify suspicious transactions for filing Suspicious Transaction Reports (STRs).

- Branches should conduct periodical review of risk categorization of accounts and apply enhanced Due Diligence measures on high risk category accounts. Such review of risk categorization of customers should be carried out at a periodicity of not less than once in six months.

- Any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of 'travelers' cheques for value of Rupees fifty thousand and above would 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.
- Cheques/drafts/pay orders/banker's cheques bearing the date or any subsequent date, if presented beyond the period of three months from the date of such instrument, would not be paid.

- Provisions of Foreign Contribution (Regulation) Act, 2010, wherever applicable, are to be strictly adhered to

- System supported monitoring of transactions will be done by the Centralized AML team at Head Office based on alerts thrown up by the AML software acquired by the Bank, or on the basis of feedback/inputs from Branches/Zonal Offices/ Circle Offices. Simultaneously, relationship points will maintain oversight over the transactions with a view to identifying suspicious transactions and bringing them to the notice of the Head Office, KYC & AML Cell.

- IBA alert indicators: Indian Banks' Association has prescribed certain indicators for generation of alerts based on report of working group on parameters for risk based transaction monitoring. The list of alert indicators for Branches/Department and alert indicators for centralized AML cell is given in **Annex- 7(a) &7(b).**

- IBA has prescribed 49 red flag indicators in respect of monitoring Trade Based Money Laundering (TBML) activities, the list of which is enclosed in Annex-7(c).

- **Fixing of Threshold Limit:**
    - Fixing threshold limit based on transaction profile of customer is one of the essential features of transaction monitoring and facilitates monitoring of transactions breaching the limit at the Branch level. The threshold limit may be reviewed and revised by GMs' Committee of AML based on the experience gained and requirement of Top Management, Government of India, RBI and other Regulatory authorities. Any transactions beyond the threshold limit fixed for the account should be looked into with extra caution.
- **Multi-level Marketing (MLM) Firms–**Accounts of Multi-level Marketing (MLM) Companies are being reportedly misused for defrauding public by luring them into depositing their money with the MLM Company by promising a high return. Such depositors are assured of high returns and issued post-dated cheques for interest and repayment of principal. So long as money keeps coming into the MLM Company's account from new depositors, the cheques

are honoured but once the chain breaks, all such post-dated instruments are dishonoured. This results in fraud on the public and is a reputational risk for banks concerned. Further, Branches should closely monitor the transactions in accounts of marketing firms. In cases where a large number of cheque books are sought by the company or there are multiple small deposits (generally in cash) across the country in one bank account or where a large number of cheques are issued bearing similar amounts/dates, Branches should carefully analyze such data and in case of such unusual operations in accounts, it is required to be reported to Reserve Bank of India and to FIU-IND, New Delhi.

- Branches 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 customer, his business and risk profile and the source of funds/wealth.

- The risk categorization of customers as also compilation and periodic Updation of customer profiles and monitoring and closure of alerts in accounts are extremely important for effective implementation of KYC/AML/CFT measures. Branches are advised to complete the process of risk categorization and compiling/updating profiles of all of their existing customers in a time-bound manner.

- The operations and transactions of the customers will be monitored on prescribed intervals taking into consideration the risk profile of the customer. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent logical or visible lawful purpose and transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer. Whenever required, Due Diligence exercise be carried out about the client's source of Funds.

- The monitoring may identify some transactions/activities of suspicious nature. These transactions/activities will be put to scrutiny through discreet and confidential enquiries. In case of suspicion, it will be reported as prescribed. The reporting will not hinder the normal operations in the account concerned by the customer. The customer will also not be informed of such reporting. Strict confidentiality has to be maintained by the Staff about its monitoring progress, reasons for suspicion and suspicious transaction reporting or otherwise for the alerts / transaction patterns observed in the customer accounts.

- Special attention shall be paid towards threats of money laundering that may arise from Inter-net Banking/Electronic Cards/Mobile Banking etc. which can be used for transfer of funds.

- After Due Diligence at the appropriate level in the Bank, transactions of suspicious nature and / or any other type of transaction notified under PML Act, 2002 will be reported to the Financial Intelligence Unit-India duly approved by Principal Officer and a record of such transactions will be preserved and maintained for a period as prescribed in the Act.

- The Branches will make use of the software for transaction monitoring and scanning the new a/c on opening and all existing a/cs in the Finacle System to ensure that no a/c is linked to any entity/ individual in the banned list circulated by U.N.

- Necessary information shall be sought about High Risk Customer's client's business & location.

5.3.1 **MONITORING OF NEWLY OPENED ACCOUNTS**

It is of utmost importance that special care is exercised while passing transactions through newly opened accounts. Special care should be exercised when a customer deposits cheques / drafts for large amounts in a newly opened current / saving account and is anxious to withdraw the amount involved or substantial part thereof quickly and in haste.

A newly opened account should remain under the close watch of the ABH of small, medium and large Branches, and the 2nd in command of other Branches, at least for an initial period of six months to guard against any fraudulent or doubtful transaction

It should be clearly understood that the concerned Branch official will be held responsible in case it transpires subsequently that such accounts have been used during the initial period of six months for fraudulent transactions.

Refund orders, dividend / interest warrants may not be accepted in newly opened accounts if the related account is opened subsequent to the date of issue of such instruments. However, refund orders, dividend / interest warrants may be accepted in accounts opened subsequent to the date of issuance of such instruments if the beneficiary has any other connected account in the same Branch opened prior to the date of issuance of such instruments. In such cases, it has to be ensured that the beneficiary is really identifiable by reference to the existing connected account(s).

Branch Manager / Senior Manager / Chief Manager may permit for acceptance of refund orders / dividend / interest warrants through account of the beneficiary which is opened subsequent to the date of issuance of such instruments provided the Branch Manager / Senior Manager / Chief Manager is satisfied about the identity of the beneficiary.

In case account number and address is also printed along with the name of the beneficiary on the refund order / dividend warrant / interest warrant, it should be ensured that the instrument is got collected in the same account of the beneficiary and the address on record with the Bank should tally with the address recorded on the instrument lodged for collection / clearance.

5.3.2 **Operation of Bank accounts and 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 some cases these third parties may be innocent while in others they may be having complicity with the criminals.

In a money mule transaction, an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times the address and contact details of such mules are found to be fake

or not up to date, making it difficult for enforcement agencies to locate the account holder.

The operations of such mule accounts can be minimised if Branches follow the guidelines on opening of accounts and monitoring of transactions as mentioned in this policy guidelines. Branches are, therefore, advised to strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical Updation of customer identification data after the account is opened and also for monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

In the circumstances when Branches believe that it would no longer be satisfied about the true identity of the account holder, it should also file an STR with FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was raised by the concerned branch, then it shall be deemed that the branch has not complied with the directions issued.

FIU-INDIA Advisory

In this regard, the FIU-IND has issued a detailed advisory dated 26.10.2023 for discouraging in opening and operations of Mule Account to prevent Cyber Enabled Frauds. FIU-India has given all its recommendations under six categories.

1: Establishment of common standard to detect and discourage Mule Accounts.

2: Sharing information across financial institutions to mitigate the migration of actors behind mule account to other bank/ institutions.

3: Implementation of Behavioural Biometrics to enhance the detection capabilities.

4: Mechanism to assign Risk score to the accounts.

5: Restricting fund flow/final withdrawal in such accounts whenever suspicious activity alert is flagged on the basis of the RFIs related to Mule Account,

6: Framework on Network Linkages of accounts through which cyber Fraud happened to trail the money to catch hold the person behind this and to return the money back to victim.

Role of Branches while Opening of Account

While opening account, Branches to scan profile of the customer. Following points to be considered:-

(a) Business/Occupation
(b) Permanent Address/Present Address
(c) Annual Income (e.g. Homemaker: Annual Receipts from spouse and for students-Annual receipts from parents to be considered).
(d) Customers having very low income should be monitored for having multiple accounts.
(e) Date of Birth
(f) Customer Risk Categorisation
(g) Verification of OVDs (in addition to verifying from original; OVDs should also be checked by downloading and searching the CERSAI portal).

(h) Biometric E-KYC of Aadhaar enabled customers.
(i) Customer behaviour in accordance to the profile of customer.
(j) Mobile number of the customer.
(k) In the account opening form, branch should that residential address columns is complete. If address in Aadhaar contains less details, alternate address proof or declaration should be insisted so that the address provided can be traced if need arises.
(l) Permanent Address and Present Address should be supported with authentic documents as per KYC norms.
(m) CKYC ID to be allotted immediately while opening of account.
(n) E-KYC to be done wherever accounts are opened through Aadhaar to enhance the accuracy and security of identity verification.
(o) Junk value/data or imaginary information should be avoided.
(p) Accounts opened by BCs should be checked meticulously by the branches.

*** Above mentioned role has been shared to branches.

For implementation of advisory of FIU-IND on detection of mule accounts and transaction monitoring on real-time at central level is under progress and subject to a machine learning and AI based technology available in peer banks/market and further consulting with FIU-IND.

As per RBI Advisory -

Suspected money mule accounts will be reflected as red flagged in Finacle system to branches for which branches may be enabled to convert the flag 'Yes/No' within turnaround time after completion of EDD. Mule account detected by branch will be restricted for debit transaction.

5.3.3 Treatment of KYC non-compliant accounts

As regards non-compliance of KYC requirements by the customers despite repeated reminders, it has been decided that Branches should impose 'partial freezing' on such KYC non-compliant a/c in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing 'partial freezing', Branches are advised 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 requirement and followed by a reminder for further period of three months. Thereafter, Branches may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts. If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing', Branches may disallow all debits and credits from/to the accounts, rendering them inoperative. Further, it would always be open to the Branches to close the account of such customers.

5.3.4 Closure of Accounts

Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such

decisions need to be taken by Branch Head.

5.3.5 **The means of establishing identity and monitoring transactions of various types of customers are enumerated herein below:**

NATURAL PERSONS:

- **Legal name and any other names** used (also known as, alias) along with father's / mother's / husband's / legal guardian's name to be ascertained from an officially valid document, such as, (a) passport, (b) PAN card, (c) voter identity card, (d) driving license with photograph, (e) Job card issued by NREGA duly signed by an officer of the State Government (vi) the letter issued by UIDAI containing details of name, address and Aadhaar number or any document as notified by the Central Government in consultation with the regulator.

  A document shall be deemed to be an "Officially valid documents" 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 a Gazette notification, indicating such change of name. [Ref: RBI notification No. DBR.AML.BC.No.46/14.01.001/2015-16 dated 29.10.2015]

- **Current and permanent residential addresses** in full (post box number should not be accepted) to be ascertained from an officially valid document which provides customer's information to the satisfaction of the Branch official authorized to open the account, such as, (a) passport, (b) voter identity card, (c) driving license (d) Aadhaar Card (e) Job card issued by NREGA duly signed by an officer of the State Government.

- Where the current address mentioned by a prospective customer in the account opening form is different from the address mentioned in the document submitted by him / her, the Branch should conduct independent verification of address of the said prospective customer by deputing an employee to the address provided by the applicant in the account opening form. The said employee shall submit a certificate, as per the Performa available at **Annex-5,** with regard to correctness of the address and the said certificate shall be attached with the account opening form.

- The Branch should mandatorily use the revised AOF & KYC forms for opening new deposit accounts.

- **Minor Accounts:** Guidelines issued by the bank from time to time should be kept in view while opening / monitoring such accounts by the Branches. However, in case a deposit account other than a current account is required to be opened in the name of minor under guardianship - whether natural or legal - full KYC procedure on the said guardian should be applied. After attaining the age of majority, the full KYC documents in respect of the minor including photograph should be obtained and entered in the system.

Institutions:

The term 'institution' includes any entity that is not a natural person. Branches need to be vigilant against business entities being used by individuals as a "front" for maintaining accounts with Banks. Branches 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 risk perception i.e. in the case of public company it will not be necessary to identify all the shareholders. Based on materiality and risk and to ascertain beneficial owners, verifications of Directors may not be taken for significant and well established entities, companies listed on recognized investment /stock exchanges, government departments or their agencies, government linked companies, statutory corporations. The detailed guidelines on the nature and type of documents or information which has to be relied upon for customer identification has been spelt out in the Bank's Manual of Instructions on Deposits which has to be followed meticulously. Moreover, guidelines issued by the Bank from time to time should be kept in view while opening /monitoring such accounts by the Branches.

The following aspect should be kept in view while opening the accounts of the institutions.

- **Sole proprietorship**

  Guidelines issued by the bank from time to time should be kept in view while opening / monitoring such accounts by the Branches, along with the norms of CAP and CIP mentioned earlier.

- **Partnership firms**

  Guidelines issued by the bank from time to time should be kept in view while opening / monitoring such accounts by the Branches. Simultaneously, KYC norms should be applied on each partner of the partnership firm so as to identify him / her individually. If any of the partners of the firm is a sleeping partner, the customer should be classified under first category, i.e., High Risk Category. In that situation, enhanced Due Diligence measures, such as, Credit Reports from the bankers of the firm(s), in which the sleeping partner plays an active role, must be obtained and transactions, particularly to and from those firms, monitored / scrutinized closely.

- **Corporate**

  Guidelines issued by the bank from time to time should be kept in view while opening / monitoring such accounts by the Branches. Latest balance sheet and profit and loss account (audited / unaudited, as may be applicable) should be obtained in order to compare the projected turnover with the past trend. In case of a new firm, sales tax /VAT return of the previous quarter(s) be obtained or the projected sales, as may be informed by the party, accepted. Bank should also monitor details of Branch offices, allied / associate concerns and nature of their business, details and nature of foreign collaboration, if any. All the Directors except Govt. Nominee Directors or nominated by Scheduled Commercial Banks/ Financial Institutions should comply with full KYC norms.

  Where a company is effectively controlled by another company ,an individual, small group of individuals or a trust, etc., the controller's identity should also be subjected to necessary KYC norms (as are applicable to the said entity) before accepting the applicant company as the customer of the Bank.

- **Thrift societies, fiduciary societies, co-operative societies, non-profit organizations etc.**

Where these entities are applicants for an account, persons exercising control or having significant influence over the organization's assets, should be considered as the principals to be identified. This will include board members, executives and account signatories. Besides, the applicant entity should also be identified separately as in the case of a corporate by obtaining proof of their legal existence, byelaws, resolution, etc. for the purpose of applying KYC norms. These accounts require enhanced Due Diligence at the time of account opening by intermediaries such as guardians of estates, executors, administrators, assignees, receivers etc. For example - the letter of administration is necessary for opening an account of administrator of the estate. The guidelines issued by the Bank in regard to opening of such accounts should be kept in view.

- **Charities, clubs, societies, religious organizations and associations**

  In case accounts are to be opened for charities, clubs, and societies, religious organizations and associations, the Branches should take reasonable steps to satisfy themselves as to the legitimate purpose of the organization by going through the constitution. The identity of the authorized signatories should be verified initially in line with the requirement of personal customers for the purpose of applying KYC norms mentioned in earlier paragraphs.

- **Hindu Undivided Family (HUF)**

  Hindu Undivided Family, as per Hindu Law, is an entity where all the members (major or minor) of a family carry on a business activity jointly and hold the property jointly.

  KYC norms should be applied on the Karta and major coparceners so as to identify each of them individually.

- **Trust accounts -**

The Branches should obtain documentation strictly as per Bank's guidelines and Due Diligence to be done, since these accounts are popular vehicles for criminals to mask the origin of criminal money they wish to launder and also avoid the identification. Branch should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/directors and the beneficiaries, if defined.And the branches shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions.

Accounts of non-face to face customers:

Apart from applying usual customer identification procedures, the Branches should follow one of the following methods of opening accounts in case meeting of the prospective customers with the authorized Branch officials is not possible:

- The prospective customers, who are having accounts with our Branches, be advised to get the Account Opening Form attested from the Branch

concerned which should also complete the required KYC norms. On receipt of such AOF, complete in all respects, directly from the Branch concerned in a sealed envelope, the accounts may be opened after observing usual safeguards.

- In other cases, i.e., where there is no Branch of our Bank at the centers where the prospective customers are stationed or they are not having accounts with our Branches at such centers, they should be advised to get themselves introduced on our prescribed AOF from their bankers. If no banker of the prospective customer is available then the party has to be present in the Branch. The said AOF, containing full particulars of the prospective customer and signatures (duly attested by the banker of the party) of the persons authorized to operate the account be got dispatched through their bankers to the Branches where accounts are to be opened. Besides, introductory letter (as per the specimen available at **Annex-6**) from the banker of the party should also be obtained as an additional safeguard. On receipt of such AOF, directly from the bank concerned in a sealed envelope, duly complete in all respects, the Branch shall get the signatures of the officials verified from the local Branch of the banker which has attested the same. In case there is no such Branch of the said banker at the center where account is to be opened, the Branch concerned shall send a letter by the quickest means of communication to the banker concerned who has introduced the prospective customer seeking confirmation about the introduction given in the AOF. On receipt of confirmation from the introducing bank and being satisfied with the introduction, the accounts may be opened by the Branch after observing usual safeguards. In no case the letter seeking confirmation from the banker of the party and the return letter containing confirmation of the banker be delivered / received from the representative of the party. Besides, other applicable documents, such as, (a)proof of identity (passport, voter's identity card, driving license, copy of PAN card), (b)proof of permanent address or current address, (c)nature of business and financial status, (d)certificate of incorporation, (e)Memorandum and Articles of Association, (f)resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf, (g)an officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf, (h)registration certificate (in case of partnership firm) (i)partnership deed, duly attested by the banker / Branch concerned, should accompany the AOF.

- In all the cases, the purpose of opening account should be categorically mentioned in the AOF by the banker of the party / our Branch concerned and the first payment to be effected through the customer's account with our Branch / another bank, which, in turn, adheres to similar KYC standards. In case such an account is opened for a specified purpose, say, for crediting proceeds of duty drawback, no other credits be accepted in such accounts. All other precautions / guidelines of opening account and operation thereof shall remain unchanged.

- Online Account opening facility: Bank has introduced online account opening facility for savings & current accounts for resident customers' wef. 27.10.2014. The precaution & risk mitigating measures to be followed by the Branches in respect of online account opening facility are given in circular No. CHO/RBD/10/2015-16 dated 19/05/2015.

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

Individual non-resident customers

Guidelines issued by the bank from time to time should be kept in view while opening / monitoring such accounts by the Branches. In case requests for opening such accounts come from persons residing outside the country, the Branches should be guided by the extant guidelines of the bank with regard to information and documents to be obtained from such persons. However, care should be taken while opening these accounts that the following documents will have to be obtained:

Passport & Residence Visa - Copies of these documents sighted in original by the Bank official or duly attested by Banker/Notary Public/Indian Embassy/ Employer to the satisfaction of the Bank.

5.3.6 SEBI Requirement

SEBI has prescribed the minimum requirement relating to KYC for certain class of the registered intermediaries from time to time after taking into account the basic principle of KYC norms or which may be prescribed by SEBI. Bank will follow the principles enshrined in the PML Act, 2002 as amended as well as the SEBI Act, 1992 as amended so that the Bank is aware of the clients on whose behalf it is dealing.

5.3.7 KYC for Existing Accounts

Branches are advised from time to time to apply the KYC norms to all the existing customers in a time bound manner. Branches should apply the KYC norms to all the new customers as well as the existing customers on the basis of materiality & risk. However, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the Customer Due Diligence measures. Branches should ensure that all the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to full KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'. Branches may also ensure that Term Deposit/Recurring Deposit accounts or accounts of similar nature are treated as new accounts at the time of renewal and subjected to revised KYC procedures.

Where the Branches are unable to apply appropriate KYC measures due to non-furnishing of information and or non-cooperation by the customer, the Branch may consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Branch Manager's permission is required before taking such decision.

Branches to ensure that mandatory entry in KYC menu in System is made in all new as well as existing customers. In customer profile all relevant fields should invariably be filled in.

5.4 RISK MANAGEMENT

The Policies and procedures put in place by the Bank for KYC/AML are to be implemented effectively. Implementation of the procedures for creating risk profiles of the existing and new customers and also the risk of various products, services,

transactions, delivery channels is to be ensured through adoption of risk based approach of this Policy.

5.4.1 Internal control system

Branch Manager of each Branch / office should explicitly allocate duties and responsibilities for opening of accounts through an office order to the staff members. Senior Officers from the Zonal Offices, during their visits to the Branches should monitor that the KYC / AML norms are being adhered to strictly as per the laid down procedures.

5.4.2 Internal audit / Compliance Function

Concurrent / Internal Auditors should specifically scrutinize and comment on the effectiveness of the measures taken by the Branches in adoption of KYC norms and the steps taken towards prevention of money laundering. Concurrent / Internal Auditors should specifically check and verify the application of KYC procedures including control being exercised by the Branches and comment on the lapses, if any, observed in this regard in their periodic inspection reports.

Zonal Office should monitor that all the eligible accounts at the Branches are fully KYC Complied

The compliance in this regard has to be put up before the Audit Committee of the Board on a quarterly basis.

A certificate from the Statutory Auditors, wherever applicable, on the compliance with KYC/AML/CFT guidelines should be obtained at the time of preparation of the Annual Statements and be kept on record.

It would be ensured that audit machinery is staffed adequately with individuals who are well-versed in KYC policies and procedures. All KYC/AML/CFT related processes, especially scrutiny and analysis of suspicious transaction alerts, would be adequately staffed with individuals conversant with KYC/AML/CFT regulation and procedures.

5.4.2.1Money Laundering and Terrorist Financing Risk Assessment by Bank.

(a) Bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise quarterly to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with bank from time to time.

(b) The risk assessment by the Bank/Branches shall be properly documented. The periodicity of risk assessment exercise shall be quarterly.

(c) The outcome of the exercise shall be put up to the audit committee of the Board, and should be available to competent authorities and self-regulating bodies.

5.4.2.2 CDD programme for mitigation and management of the identified risk

Branches shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment), controls and procedures in this regard. Branches shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, Branches shall monitor the implementation of the controls and enhance them if necessary.

5.4.3 CUSTOMER RISK CATEGORIZATION (CRC)

It is mandatory for banks in India to introduce a system of CRC for their customers. 'Customer risk' in the present context refers to the money laundering risk associated with a particular customer from a bank's perspective. This risk is based on the risk perceptions associated with the parameters comprising a customer's profile, and the level of risk associated with the product and channels being used by him.

To parameterize risk perception of the customer in terms of nature of business/ activity, location of customer, mode of payments, volume of turnover, social and financial status, etc to enable categorisation of customers into low, medium and high risk.

Classify customers into various risk categories such as high, medium and low risk and based on risk perception, decide on acceptance criteria for each category of customers; Review of risk classification to be done at specified interval or if there is a material change in the customer profile.

The customer profile may contain information relating to customer's identity, location, social/financial status, nature of business activity, volume of turnover, mode of payment, information about his clients' business and their location in case of any materiality and risk perceived, etc. The nature and extent of Due Diligence will depend on the risk perceived by the bank. However, while preparing Customer profile, Branches should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes except when such details are sought by Regulatory/Statutory Authorities.

The Bank has adopted policy for Risk Categorisation of customers based on the following parameters as approved by the Committee of General Managers/Executives, authorized by the MD&CEO**;**

Customers Identity: Customer Constitution

Social /Financial Status: Net worth of customer

Nature of business Activity: Customer Occupation

- Products
- Services/Delivery
- High ML risk countries as per FATF
- Customers' locations

Based on the above criteria, the customers have been categorized into three types of risk categories i.e. high, medium and low risk. The System will assign the Risk category of every customer based on the above criteria on real time basis. Branch

should note the Risk Category of customers in the Account opening forms after creation of Customer Id. The risk category of customers will be reviewed by the system on quarterly basis. However, the customer should not know the category of risk in which he /she /entity has been placed by the Branch.

5.4.3.1 High Risk:

The following types of customer to be treated as High Risk:

- Customers those engaged in certain profession where Money Laundering possibilities are high i.e. Antique Dealers (individual & entities), Money Services Bureau (entities - not employees of these entities) and dealers in arms etc.
- Persons who live in High AML Risk countries (nationality is irrelevant). An indicative list of High Risk countries is available at **Annex-9.**
- Firms with "Sleeping Partner (s)".
- Politically Exposed Persons (PEPs) of foreign origin (Individuals who are or have been entrusted with prominent public functions in a foreign country, for example, heads of states or of governments, senior politicians, senior government / judiciary / military officers, senior executives of state-owned corporations, important political party officials, etc.)Close relatives, such as, father, mother, brother, sister, spouse, son, Daughter, father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law, stepfather, stepmother, stepbrother and stepsister of the politically exposed persons.
- Trusts, charities, NGOs, NPOs, religious / social organizations and the organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies).
- Where accounts are opened/operated through a mandate or power of attorney.
- Persons/entities with dubious reputation as per the information available in public domain.
- Non face-to-face customers.
- Countries which have been following indicative characteristics without adequate anti-money laundering standards and regulations; or where there is a politically unstable regime with high levels of public or private sector corruption; or that are known to be drug producing or drug transit countries; or that have been classified by Financial Action Task Force as non-cooperative countries and territories.
- Companies having close family shareholding or beneficial ownership.
- Nonresident customers and foreign nationals.
- High Net worth customers as given in the **Annex-10.** The para-meterization for identifying HNI shall be kept under review. The opening of accounts of such category of persons would require specific approval of Branch heads.
- Multi-Level Marketing Companies account.

- Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.
- Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities.
- Individuals and entities in watch lists issued by Interpol and other similar international organizations.
- Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk.
- Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institution, frequent and unexplained movement of funds between institution in various geographic locations etc.
- Off-shore (foreign) corporation/business
- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
- Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.
- Investment Management/Money Management Company/Personal Investment Company
- Accounts for 'gatekeepers' such as accountants, lawyers or other professionals for the clients where the identity of the underlying client is not disclosed to the financial institution.
- Client Accounts managed by professional service providers such as law firms, accountant, agents, brokers, fund managers, trustees, custodians etc.
- Money Service Business: Including seller of: Money Orders/Travelers' Cheques/Money Transmission/Check Cashing/Currency Dealing or Exchange.
- Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques/cash payroll checks).
- Gambling/gaming including' Junket Operators' arranging gambling tours.
- Dealers in high value or precious goods (e.g. Jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
- Customers engaged in a business which is associated with higher levels of corruption e.g. arms manufacturers, dealers and intermediaries.

- Customers engaged in industries that might relate to nuclear proliferation activities or explosives.

5.4.3.2 Medium Risk:

Customers who are likely to pose a higher than average risk to the bank should be categorized as Medium Risk Customer.

- Any of the accounts holders or the owners / controllers living in a Medium Risk country (Nationality is irrelevant). An indicative list of Medium Risk countries is available at **Annex-9.**
- Current Account customers where credit or debit summations exceed Rs.50 lakh per annum in their accounts but they do not provide sufficient documentary proof {viz.(i) balance sheet, profit and loss account, or Receipt and payment of funds, income and expenditure statement, or Income tax returns / assessment order, as the case may be}.
- Other deposit account customers where credit or debit summations exceed Rs.10 lakh per annum in their accounts but they do not provide sufficient documentary proof, such as, salary slip, income tax return/assessment order, etc.
- Non-Bank Financial institution
- Stock brokerage
- Import/Export
- Gas Station
- Car/Boat/Plane Dealership
- Electronics (wholesale)
- Travel agency
- Used car sales
- Telemarketer
- Providers of telecommunications service, internet cafe, IDD (International Direct Dialing) call service, phone cards, phone center
- Dot-com company or internet business
- Pawnshops
- Auctioneers
- Cash-intensive Business such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
- Sole Practitioners or Law Firms (small, little known)
- Notaries (small, little known)
- Secretarial (small, little known)
- Accountants (small, little known firms)

- Venture capital companies

5.4.3.3 Low Risk:

Individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts, by and large, conform to the known profile may be categorized as low risk customer.

- Salaried employees whose salary structures are well defined.
- People belonging to lower economic strata of the society whose accounts show small balance and low turnover.
- Government Departments.
- Government owned companies, regulator & statutory bodies etc.
- All borrowal customers (other than high risk category) where Due Diligence is done at the time of granting the facilities.
- All customers not falling under the category of High and Medium Risk can be classified under Low Risk Category.
- NPOs/NGOs promoted by United Nations or its agencies.

5.4.3.4 Exempted categories:

- Scheduled commercial banks, local bodies, government departments, public sector undertakings or quasi-government bodies.

5.4.4 Review of Risk Categorization:

Branches to review risk categorization of accounts and the need for applying enhanced Due Diligence measures as & when the risk perception changes & the same to be reported to HO, KYC& AML cell for effecting such changes in the system**.** However, routine half yearly review of risk category of customers will be carried out by DIT.

The Risk Parameters/ benchmarks on customers risk categorization may be reviewed by a Committee of General Managers, as authorized by the MD&CEO/ED.

5.4.5 Periodic Updation of KYC

A risk-based approach should be adopted for Periodic Updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, Periodic Updation should be carried out at least once in every 10(ten) years in case of Low risk Customer, once in every 8(eight) years in case of Medium Risk Customer and once in every 2(two) years for High Risk Customers as per the following procedures.

(1)Individual Customers:

(a)No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter etc**.(Annex-22)**

(b) Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.Further, Banks/branches may obtain a copy of OVD or deemed OVD or the equivalent e-documents for the purpose of proof of address, declared by the customer at the time of periodic updation **(Annex-23).**

(c) Accounts of customers who were minor at the time of opening account on their becoming major: In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the bank/branch. Wherever required, branches may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

(d) Aadhaar OTP based e-KYC in non-face to face mode may be used for Periodic updation.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Bank/branches shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

(2). Customers other than individuals:

(a) No change in KYC information: In case of no change in the KYC information of the LE (legal entity) customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of the bank, letter from an official authorized by the LE in this regard, board resolution etc. Further, bank/branches shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-date as possible**.(Annex-25)**

(b).Change in KYC information: In case of change in KYC information, branches shall undertake the KYC process equivalent to that applicable for on-boarding a new LE (Legal Entity) customer.

(3). Additional measures: In addition to the above, Bank/Branches shall ensure that

(a).The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the branch are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the branch has expired at the time of periodic Updation of KYC, branches shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

(b). Customer's PAN details, if available with the bank/branch, is verified from the database of the issuing authority at the time of periodic Updation of KYC.

(c). An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic Updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic Updation of KYC are promptly updated in the records / database of the bank and an intimation, mentioning the date of Updation of KYC details, is provided to the customer.

(d). In order to ensure customer convenience, the facility of periodic Updation of KYC to be provided at any branch. Branches to ensure that processes on Updation/ periodic Updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

(e) CDD as specified in section No.5.2.2 to be carried out.

(f) Certified copy of OVD containing identity and address shall be obtained at the time of periodic Updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorized as 'Low' risk. In case of low risk customers when there is no change in status with their identities and addresses, a self – certification to that effect shall be obtained

(g) In case of Legal entities, Branch should review the documents sought at the time of opening of account and obtain fresh certified copies. Provided, Branch shall ensure that KYC documents, as per extant requirements of the KYC & AML Policy, are available with them.

(h) Branches should not insist requirement of obtaining recent photograph or the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder(s) is required to establish their bona-fides.

The time limit prescribed above will apply from the date of opening of account/last verification of KYC.

(4) Banks shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the bank/branches the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at the Bank end.

.

Further, In terms of RBI notification RBI/2021-22/29 DOR. AML.RE 13/14.01.001/202122 dated May 5, 2021, keeping in view the current COVID-19 related restrictions in various parts of the country, branches are advised that in respect of the customer accounts where periodic Updation of KYC is due and pending as on date, no restrictions on operations of such account shall be imposed till December 31, 2021, for this reason alone, unless warranted under instructions of any regulator/ enforcement agency/court of law, etc.

The relaxation provided till December 31, 2021 is extended till March 31, 2022 in line with RBI Circular RBI/2021-22/144 DOR.AML.REC.74/14.01.001/2021-22 Dated December 30, 2021

However, branches are also advised to continue engaging with customers for having their KYC updated in such cases.

(4) <u>Partial freezing of transactions in non-complied customers due for REKYC</u>

a) First Notice- Prior to 90 days of due date of RE-KYC, 30 days notice will be made available to branch in Finacle system. Branch will dispatch the notice to customer within 07 days by registered post/speed post or authentic courier service and the ID number issued by Post Office/Courier Service should be seeded in Finacle system by branch otherwise day end of branch will be restricted automatically by the Central Server.

b) Second Notice- Prior to 60 days of due date of RE-KYC, 30 days notice will be made available to branch in Finacle system. Branch will dispatch the notice to customer within 07 days by registered post/speed post or authentic courier service and the ID number issued by Post Office/Courier Service should be seeded in Finacle system by branch otherwise day end of branch will be restricted automatically by the Central Server.

c) Third or Final Notice- Prior to 30 days of due date of RE-KYC, 30 days notice will be made available to branch in Finacle system. Branch will dispatch the notice to customer within 07 days by registered post/speed post or authentic courier service and the ID number issued by Post Office/Courier Service should be seeded in Finacle system by branch otherwise day end of branch will be restricted automatically by the Central Server. After sending the final notice to customer, account will be frozen for debit transaction on due date of RE-KYC or expiring date of notice whichever is later.

5.4.5.1Updation of PAN of Existing Customer

In case of existing customers, Branch 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 Branch 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 Branch shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, If Customer is 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; **Branch shall send the details seeking permission for relaxation(s) of continuing operations in such accounts to Zonal office and Zonal office may allow such relaxations for continuing operations in the account based on merit of the accounts.**, Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship

with a Branch gives in writing to the Branch that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, Branch 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 Bank 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.

6. Officially valid documents under PML rules.

A. The following documents are the Officially Valid Documents (OVDs) as per PML Rules**:**

- (i) Passport (ii) Driving License (iii) Voter's Identity Card issued by Election Commission of India(iv) Proof of Possession of Aadhaar (v) Job card issued by NREGA duly signed by an officer of the State Government (vi) The letter issued by the National Population Registrar containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator

- E-KYC service of Unique Identification Authority of India (UIDAI) may 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 may be treated as an 'Officially Valid Document'. However, the individual user has to authorise to UIDAI, by explicit consent, to release her or his identity / address through biometric authentication to the Branch.

- Further, e-Aadhaar downloaded from UIDAI website may be accepted as an officially valid document subject to the following:

    - If the prospective customer knows only his/her Aadhaar number, the Branch may print the prospective customer's e-Aadhaar letter in the Branch directly from the UIDAI portal or adopt e-KYC procedure as mentioned in paragraph (b).

    - If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the Branch may print the prospective customer's e-Aadhaar letter in the Branch directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in paragraph (b) above; or confirm identity and address of the resident through simple authentication service of UIDAI.

- An indicative list of the nature and type of documents / information that may be relied upon for customer identification is given in Annex-1**.** It is clarified that permanent correct address, as referred to in Annex-1, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the bank for verification of the address of the customer. If the address on

the document submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document may be accepted as a valid proof of both identity and address If the address indicated on the document submitted for identity proof differs from the current address mentioned in the account opening form, a separate proof of address would be obtained. A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address.

- Where a Passport is taken as evidence of identity, the number, date and validity period & country of issue should be recorded.
- The indicative list as furnished in Annex-1 is not to be treated as an exhaustive list. Branches are, therefore, advised to be guided by the instructions issued by our bank from time to time in this regard.

7. Implementing Unique Customer Identification Code (UCIC):

The increasing complexity and volume of financial transactions necessitate that customer do not have multiple identities within a bank, across the banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer. The Unique Customer Identification Code (UCIC) will help Branches to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers. UCIC would be allotted to all customers while entering into new relationships.

Branches to ensure that unique Cust-id is allocated to new accounts as well as existing accounts in line with RBI guidelines. 'CUSTOP' menu is to be invariably invoked while creating a new Cust-id. Branches should check in system through **y** search menu, if the prospective/existing customer is having multiple Cust-ids based on common fields [PAN, Aadhaar, Passport, and Mobile No**. ,** Driving License, MNREGA, Voter ID card]. In such cases, only one unique Cust-id is to be allocated by merging other multiple Cust-ids.

8. e-KYC service of UIDAI :

In order to reduce the risk of identity fraud, document forgery and to have paperless KYC verification, UIDAI has launched its e-KYC service. 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, 2005. Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") may be treated as an 'Officially Valid Document' under PML Rules.

While using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent to release her or his identity/address through biometric authentication to the bank Branches/ business correspondents (BCs). The UIDAI then transfers the data of the individual comprising name, age, gender, and photograph of the individual electronically to the Bank/BCs which may be accepted as valid process for KYC verification.

Physical Aadhaar card issued by UIDAI containing details of name, address and Aadhaar number would continue to be accepted as an 'officially valid document' for KYC.

M/S CSC(Common Service Center) e- Governance is the system integrator of our Bank for Aadhaar E-KYC authentication service and provides user DATA to registered clients. CSC Has a KSA (KYC service Agency) relationship with UIDAI. Branches can log in to https://aua.csc.gov.in/kycweb in Google Chrome browser. Details of procedure are furnished in letter no. HO/FI/445/2013-14 dated 09.01.2015.

9. Centralized KYC Records Registry (CKYCR

The Government of India vide their Notification dated November 26, 2015 authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as and to perform the functions of the Central KYC Records Registry under the PMLA rules, including receiving, storing, safeguarding and retrieving the KYC records in digital form of a "client", as defined in clause (ha) of sub-section (1) of Section 2 of the Prevention of Money-Laundering Act, 2002.

Central KYC Records Registry is a centralized repository of KYC records of customers in the financial sector with uniform KYC norms and inter-usability of the KYC records across the sector with an objective to reduce the burden of producing KYC documents and getting those verified every time when the customer creates a new relationship with a financial entity.

In terms of provision of Rule 9(1A) of PML Rules, the Branches shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR): -

Branches to enter the KYC information as per new KYC application form for individuals and Legal entities as the case may be and scan the KYC documents i.e., ID & address proof along with Signature & photograph for Individual accounts w.e.f 01.01.2017 for uploading to CKYCR. Branches may download the KYC documents on the basis of CKYC Identifier for opening accounts of Individual customers. Branches are, however, allowed time up to February 1, 2017 for uploading data in respect of accounts opened during January 2017.

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

Branches shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

Once KYC Identifier is generated by CKYCR, Bank/Branches shall ensure that the same is communicated to the individual/LE as the case may be.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Branches shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the Implementation date at the time of periodic

Updation as specified in KYC AML Policy of the bank, when the updated KYC information is obtained/received from the customer.

Branches shall ensure that during periodic Updation, the customers are migrated to the current CDD standard.

Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to Bank/Branch, with an explicit consent to download records from CKYCR, then such Bank/Branch shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

1. There is a change in the information of the customer as existing in the records of CKYCR;

2. The current address of the customer is required to be verified;

3. The Bank/Branches considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

4. The validity period of documents downloaded from CKYCR has lapsed.

10. Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

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.

Foreign Accounts Tax Compliance Act (FATCA) is a US legislation aimed at tackling tax evasion by US persons holding investment in accounts outside US. FATCA requires Foreign Financial Institutions (FFI) to report information related to the ownership by U.S. persons of assets held at overseas.

Govt. of India has since signed the Inter-Governmental Agreement (IGA) on 9th July, 2015 with USA for improving International Tax compliance and implementing the FATCA. In this regard Government of India, Ministry of Finance, Department of Revenue, Central Board of Direct Taxes has notified the rules vide notification S.O. 2155(E) dated 7th August, 2015.

The information required to be captured in respect of FATCA reportable customers are incorporated in our revised KYC application forms as well as in our CBS system.

The compliance & reporting under FATCA is done by International Department, Head Office.

11. INTRODUCTION OF NEW TECHNOLOGIES - CREDIT CARDS / DEBIT CARDS / SMART CARDS / GIFT CARDS

Branches/Offices should pay special attention to any money laundering threats that may arise from new or developing technologies including Internet Banking, Mobile Banking etc. that might favor anonymity. The Branches/ Controlling Data Centre should not provide internet facility to any person without opening an

account and compliance of applicable KYC norms. The Branches should also ensure that the amount transferred /received through electronic mode, beyond a threshold limit, as may be in vogue, should be by debiting/crediting the accounts of the customers concerned.

The Branches should ensure that full KYC procedures/compliance are duly applied before issuing Debit Cards/Smart cards/Gift Cards in respect of add-on/supplementary card holders also.

The Branches/offices should ensure that the Agents, if any, engaged or appointed for the purpose of marketing of any product (including delivery to the customers),are also subjected to KYC procedures.

12. ADHERENCE TO FOREIGN CONTRIBUTION AND REGULATION ACT (FCRA) 2010

Branches shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made there under. Further, branches shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India.

13. ADHERENCE TO GUIDELINES FOR AUTHORISED MONEY CHANGERS

Authorized Branches undertaking the business of moneychanger should adhere to the provisions of Anti-Money Laundering guidelines of the Reserve Bank of India issued from time to time. The Prevention of Money Laundering (Amendment) Act, 2009 has defined and included 'Authorized Persons' and 'Payment System Operators'. As per RBI's directions, all the KYC norms /AML standards /CFT/Obligations of APs (Money Changing Activities)/Payment System Operators shall be adhered to. In case of 'Authorized Persons' a certificate from the Statutory Auditors on the compliance with KYC/AML/CFT guidelines should be obtained at the time of preparation of the Annual Closing and kept on record.

14. Combating Financing of Terrorism (CFT):

In order to have control and effective monitoring of suspicious transactions which gives rise to a reasonable ground of suspicion involving financing of the activities relating to terrorism, it is essential to have proper record for monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the FIU-IND on priority.

Branches must ensure that before opening a new account the name(s) of the proposed customer does not appear in the list of individuals and banned entities as circulated by Reserve Bank of India, which is further being forwarded by HO to Branches through Zonal Offices and also available at the United Nations website: https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/1267.pdf

Branches should scan all existing accounts to ensure that no account is held with link to any of the entities or individuals included in the list. It is the responsibility of the Branches that full details of accounts bearing resemblance with any of the individuals / entities in the list should immediately be intimated to their Zonal Office and in-turn Zonal Office to intimate Circle Office/Head Office for onward reporting to Reserve Bank of India and FIU-IND.

15. Freezing of Assets under sec 51A of Unlawful Activities (Prevention) Act 1967

(i) Requirements/obligations under International Agreements Communications from International Agencies –

Bank 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

www.un.org/securitycouncil/sanctions/1267/aq sanctions list

(b) The " Taliban Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at

https://www.un.org/securitycouncil/sanctions/1988/materials

(ii) 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 **February 2, 2021.**

(iii) 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.

(iv) 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.

Branches are required to strictly follow the procedure laid down in the UAPA Order dated **February 2, 2021(Annex-11) and detailed as in section 15.1 of this policy guideline** and ensure meticulous compliance to the Order issued by the Government. Updated reference is also available in RBI circular: **RBI/2023-24/50 DOR.AML.REC.26/14.06.001/2023-24 dated July 24, 2023**.

15.1 Unlawful Activities (Prevention) Act, 1967: Procedure to be adopted by Bank/Branches.

In relation to compliance with the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purposes of prevention of and for coping with terrorist

activities, the Bank shall perform the following:-

(i) Where the particulars of any of the Bank's customers match with the particulars of designated individuals/entities, Branch shall report through Zonal Office 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, held by such customer on their bookstotheJointSecretary,CounterTerrorismandCounterRadicalizationDivision (CTCR Division), Ministry of Home Affairs (MHA), by fax No. 011-23092551 and also convey the same over telephone on 011-23092548. The particulars, apart from being sent by post / fax/ telephone, shall necessarily be conveyed on e-mail id: jsctcr-mha@gov.in under copy to the KYC-AML cell ,HO e-mail id: ho.kycaml@ucobank.co.in

(ii) The KYC-AML Cell of the Bank shall also send by post a copy of the communication mentioned in (i) above to the UAPA Nodal Officer of RBI, Chief General Manager, Department of Banking Operations and Development, Anti Money Laundering Division, Central Office Building, 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai-400 001 and also by fax. The particulars apart from being sent by post / fax shall necessarily be conveyed by e-mail by the KYC-AML cell.

(iii) The KYC-AML Division of the Bank shall also send a copy of the communication mentioned in (i) above to the UAPA Nodal Officer of the State/UT where the account is held as the case may be and to FIU-India.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is **beyond doubt**, the branches shall prevent designated persons from conducting financial transactions, under intimation to Joint Secretary, Counter Terrorism and Counter Radicalization Division (CTCR Division), Ministry of Home Affairs, by fax and also convey over telephone. The particulars apart from being sent by post shall necessarily be conveyed by e-mail.

The KYC-AML Cell shall also file a Suspicious Transaction Report (STR) with FIU- IND covering all transactions in the accounts covered by paragraph (i) above, carried through or attempted, as per the prescribed format.

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. The list of Nodal Officers for UAPA is available on the website on Ministry of Home Affairs.

15.2 Freezing of financial assets:

On receipt of particulars as mentioned in preceding paragraphs, Counter TerrorismandCounterRadicalizationDivision(CTCRDivision)ofMHAwouldgetthemverified.In case, the results of the verification conducted by the MHA (through State Police and / or the Central Agencies) 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 under intimation to Reserve Bank of India and FIU-IND.

Procedure as enumerated in Clause15.1 shall also be followed on receipt of information/request from the RBI. The order shall take place without prior notice to the designated individuals /entities.

15.3 Procedure for unfreezing of Financial Assets

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 Bank. The KYC-AML Division shall inform and forward a copy of the application together with full details of assets 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 Joint Secretary, Counter Terrorism and Counter Radicalization Division (CTCR Division) of MHA through Fax/ telephone/ e-mail within two working days. The Nodal Officer shall get it verified based on the basis of evidence furnished by the individual / entity and if he is satisfied, he shall pass an order unfreezing the funds, financial assets or economic resources or related services owned/ held by such applicant under intimation to the concerned bank.

15.4 Communication of Orders under Section 51A of the Unlawful Activities (Prevention) Act

All Orders under Section 51A of the Unlawful Activities (Prevention) Act, relating to the Funds, Financial Assets or Economic Resources or Related Services, would be communicated to all banks through RBI.

15.5 Countermeasures

Branches shall undertake counter measures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

16. Jurisdictions that do not or insufficiently apply the FATF Recommendations:

Branches 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. Branches shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF. 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.[FATF Statements are circulated by Reserve Bank of India from time to time].

17. Correspondent Banking :

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 arrangement for demand drafts and mail transfers, payable-through-accounts, cheque clearing etc. It is emphasized that sufficient information should be gathered to understand fully the nature of the business of the correspondent / respondent bank. Information of other bank's 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 correspondent's / respondent's country may be of special relevance. It will also be important to determinefrom publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action and also assess the respondent bank's AML/CFT controls. Further, Correspondent relationship shall not be entered into or continued with a shell bank.

While it is desirable that such relationships should be established only with the approval of Competent Authority so delegated under approved policy of the Board laying down clear parameters for approving such relationships. Proposals approved should invariably be put up to the Board at its next meeting for post-facto approval, as per directions from Reserve Bank of India.

In view of what has been stated above, it will be essential for our Bank to obtain necessary information on observance of KYC norms with whom our Bank will be entering into correspondent / respondent relationship whether it is within the country or outside the country. Therefore, the Branches, Zonal Offices and Corporate Offices should clearly understand the nature of relationship with which they will be entering into with other banks and whether they are KYC compliant or otherwise. This will help the bank in safeguarding its interest.

The information can be obtained either by writing to the banks concerned with whom we shall be entering into any kind of relationship or obtain the information from the public domain whichever is easily accessible. It has to be ensured that the responsibility with whom correspondent / respondent relationship is established, is clearly defined/documented. In case of payable-through-accounts, particularly

the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the account and is undertaking ongoing 'Due Diligence' on them. Wherever we are the correspondent bank, we should ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

In order to comply with the applicable laws & regulations, we are required to obtain information regarding the procedures for fighting Money Laundering & "Know Your Customer" from other Financial Institutions, who are dealing with us. For this purpose, the functional department has to procure information as per questionnaire form which should be kept on record for inspection by the Regulatory Authorities **(Annex-12).**

At par facility offered to Cooperative Banks:

Some Branches may have arrangements wherein they will be approached by Cooperative Banks for the arrangement to open current accounts with the Branches and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in-customers for facilitating their remittances and payments. This 'at par' facility to co-operative banks would be in the nature of correspondent banking arrangements.

Therefore, Branches/offices are advised to monitor and review such arrangements to assess the risks including credit risk and reputational risk arising there from and also Branches/offices should retain the right to verify the records maintained by the client cooperative banks/societies for compliance with the extant instructions on KYC/AML under such arrangements. [Reserve Bank of India circular No. DBOD.AML.BC.No.81/14.01.001/2015-16 dated 25th Feb 2016]

Correspondent relationship with a "Shell Bank"

A 'Shell Bank' is defined as a Bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

Shell Bank is not permitted to operate in India. Therefore, it becomes imperative that we should take necessary guard against establishing relationship with respondent foreign financial institutions that permit their accounts to be used by Shell Banks. We should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Functional Department (HO International Wing) should ensure that respondent banks have anti-money laundering policy and procedures in place and apply enhanced 'Due Diligence' procedures for transactions carried out through the correspondent accounts.

Branches and Subsidiaries outside India:

The extant guidelines shall apply to the Branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF recommendations, to the extent local laws permit. In case there is a variance in KYC/AML standards prescribed by RBI and the Host country regulators, Branches/overseas subsidiaries are required to adopt the more stringent regulation of the two. Besides, when local applicable laws & regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank.

18. Foreign Portfolio Investors (FPIs)

FPIs have been categorized by SEBI based on their perceived risk profile as detailed in **Annex-13**. 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-14**) subject to Income Tax (FATCA/CRS) Rules would be required. For this purpose, banks 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 Rules.

In this regard, SEBI has been requested to advise Custodians/Intermediaries regulated by them to share the relevant KYC documents with the banks concerned based on written authorization from the FPIs. Accordingly, a set of hard copies of the relevant KYC documents furnished by the FPIs to the Custodians/Regulated Intermediaries may be transferred to the bank concerned through their authorized representative. While transferring such documents, the Custodian/Regulated Intermediary shall certify that the documents have been duly verified with the original or notarized documents have been obtained, where applicable. In this regard, a proper record of transfer of documents, both at the level of the Custodian/Regulated Intermediary as well as at the bank, under signatures of the officials of the transferor and transferee entities, may be kept. While opening bank accounts for FPIs in terms of the above procedure, banks may bear in mind that they are ultimately responsible for the customer Due Diligence done by the third party (i.e. the Custodian/Regulated Intermediary) and may need to take enhanced Due Diligence measures, as applicable, if required. Further, banks are required to obtain undertaking from FPIs or Global Custodian acting on behalf of the FPI to the effect that as and when required, the exempted documents as detailed in **Annex-14** will be submitted.

It is further advised that to facilitate secondary market transactions, the bank may share the KYC documents received from the FPI or certified copies received from a Custodian/Regulated Intermediary with other banks/regulated market intermediaries based on written authorization from the FPI.

19. Wire Transfers:

Banks use wire transfer 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 country. As Wire Transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

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

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 may be the same person.

- 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.

- 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 analyzing suspicious or unusual activity and disseminating it as necessary. 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.

19.2 Cross-border wire transfers

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.

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

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.

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 mentioned.

19.3 Domestic wire transfers

Domestic wire transfer means any wire transfer where the Originator Bank and Beneficiary Bank 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.

All domestic wire transfers of Rs.50000/-(Rupees Fifty Thousand) and above should be made through accounts and must include complete originator information i.e. name, address and account number etc.

If bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs.50000/-(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.

In case of domestic wire transfers below Rs. 50000/- (Rupees fifty thousand) where the originator is not an account holder of the ordering bank and where the information accompanying the wire transfer can be made available to the beneficiary bank and appropriate authorities by other means, it is sufficient for the ordering bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

The ordering bank shall make the information available within three working / business days of receiving the request from the intermediary bank, beneficiary bank, or from appropriate competent authorities.

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

19.4 Exemptions

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

19.5 Role of Ordering, Intermediary and Beneficiary banks

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 ten years.

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.

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.

19.6 Serial Payment:

It refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering bank to the beneficiary bank directly or through one or more intermediary financial institutions (e.g., correspondent banks).

19.7 Straight-through Processing:

It refers to the payment transactions that are conducted electronically without the need for manual intervention.

19.8 The wire transfer instructions are not meant to cover the following types of payments:

- Any transfer that carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), for the purchase of goods or services, the reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.
- Interbank transfers and settlements, where both the originator person and the beneficiary person are regulated by bank acting on their own behalf.

19.9 Money Transfer Service Scheme (MTSS)

MTSS providers are required to comply with all of the relevant requirements of this Section, whether they are providing services directly or through their agents. Banks that control both the ordering and the beneficiary side of a wire transfer shall:

- take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
- file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.

19.10 Other Obligations :

a) Obligations in respect of bank' engagement or involvement with unregulated entities in the process of wire transfer

- Banks in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned bank shall be fully responsible for information, reporting and other requirements and therefore shall ensure that.

  i) There is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved.
  ii) the agreement / arrangement, if any, with such unregulated entities, banks clearly stipulates the obligations under wire transfer instructions.

iii) Termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

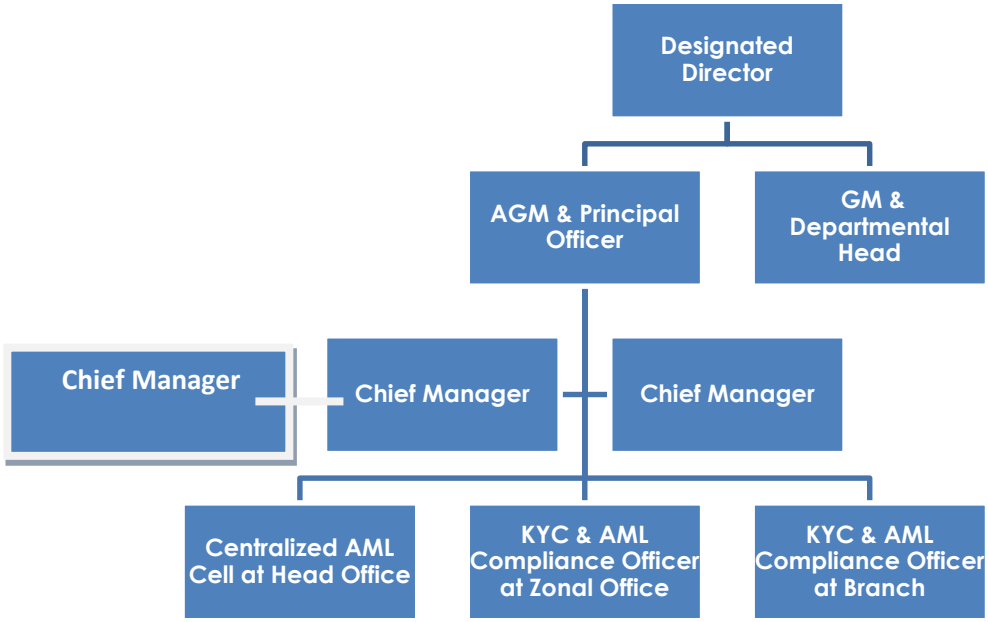
b) Bank's responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities)

Banks are prohibited from conducting transactions with designated persons and entities

c) Bank's responsibility to fulfill record management requirements

Complete originator and beneficiary information related to wire transfers shall be preserved.

20. Hierarchy of AML control and Monitoring:



21. Designated Director

With the enactment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act which provides for "Powers of Director to impose fine", the section 13(2) now reads as under:

"If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—

a) issue a warning in writing; or

b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

d) By an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."

In view of the amendment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act, [RBI Circular No. DBOD.AML.BC.No.80/14.01.001/2013-14 dated December 31, 2013] banks are to nominate a Director on their Boards as "designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012.

As per new definition of Designated Director (Rule 2(ba) of PML Act):"Designated Director" means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and shall be nominated by the Board and includes --

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

b) the managing partner if the reporting entity is a partnership firm,

c) the proprietor if the reporting entity is a proprietorship concern,

d) the managing trustee if the reporting entity is a trust,

e) 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

f) 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.

Accordingly, Executive Director of our Bank has been nominated as "Designated Director" for the same.

As per Rule 7(1) of PML Act, 2002, the name, designation and address of the Designated Director is to be communicated to Director, FIU-IND. In addition, it shall be the duty of every reporting entity (i.e. Bank), its designated Director, officers and employees to observe the procedures and manner of furnishing and reporting information on transactions referred to Rule3 in PML Rules.

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

22. Senior Management

As per Master Direction on KYC of RBI (Chapter-II, Point-8), Bank has to specify as to who constitute Senior Management for the purpose of KYC compliance.

Accordingly, Chief Manager and above be identified as Senior Management for the purpose.

23. Principal Officer

An Officer of sufficient seniority, competence and independence must be appointed Principal Officer who has sufficient level of seniority within the Bank and has sufficient resources, sufficient time and support staff to ensure that - (a) day to day operation in context of Anti Money Laundering Policy is monitored, (b) responding promptly to any inquiry/ies from the regulators, (c) receive internal suspicious activity reports, (d) reasonable steps taken to access any relevant KYC information, (e) obtaining and using National and International findings concerning countries with inadequacies in their approach to money laundering prevention, (f) making requisite external reports and (g) taking reasonable steps to establish awareness, and staff training.

It has to be ensured that the Principal Officer is able to act independently and report directly to the Senior Management or to the Board of Directors. The Principal Officer should also be responsible for developing appropriate compliance management arrangements across the full range of KYC/AML/CFT areas.

Principal Officer" means an officer at the management level nominated by the bank, responsible for furnishing information as per rule 8 of the Rules.

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

23.1 Responsibilities of Principal Officer:

Principal Officer will be responsible for

- Ensuring Compliance, Monitoring Transactions and Implementation of the KYC-AML -CFT Policy.
- Sharing and reporting information as required under the law/regulations.
- Maintaining close liaison with enforcement agencies, and banks and any other institution which are involved in the fight against Money Laundering and Combating Financing of Terrorism (CFT).
- Ensuring submission of cash Transaction Report (CTR), Cross Border Wire Transfer Reports (CBWTR) and Non-Government Organization / Non-Profit Earning Organization Report (NTR) to FIU-IND, New Delhi within 15 days of every succeeding month.
- Ensuring submission of suspicious Transaction Report (STR) to FIU-IND, New Delhi within seven days from the date of arriving at conclusion that transaction is suspicious.
- Ensuring submission of Counterfeit Currency Report (CCR) to FIU-IND, New Delhi within 15th of subsequent month of the date of detection and reporting by Branches through GAD.
- Ensuring Monthly Reporting of the CTRs/NTRs/STRs/CCRs to FIU-IND, New Delhi and about implementation of KYC-AML-CFT policy in the bank to the Top Management.
- Ensuring Updation /revision of KYC-AML-CFT policy of the bank by incorporating guidelines/instructions issued by Reserve Bank of India from time to time.

- Ensuring compliance of Regulatory Guidelines/Instructions and obligation of bank under PML Act, 2002 **(Annex-15).**

23.2 Assistance /Support to the Principal Officer

Role and responsibilities of functional departments at Head Office

Principal Officer will be assisted by KYC-AML Cell.

The support role, domain and responsibilities of functional departments at Head Office to ensure proper implementation and adherence, across the bank, to KYC norms/ AML standards/Combating of Financing of Terrorism (CFT)/ obligations of banks under Prevention of Money Laundering Act, PMLA, 2002 as amended by Prevention of Money Laundering (Amendment Act), 2009, has been identified as below.

24. Role and responsibilities of different departments of Head Office for KYC / AML Compliance

Department	Functions
KYC & AML Cell, Compliance Department, Head Office	• Policy formulation and procedural guidelines in consonance with directives from Regulatory/Statutory Authorities. • Scrutinizing of STR alerts by designated Money Laundering Reporting Officers (MLROs) of the AML cell • Supervision of scrutiny of alerts done by Money Laundering Reporting Officers (MLROs), Screening of marked STRs by Money Laundering Reporting Officers (MLROs) and SARs received from Branches. • Placing of possible STRs to AML Screening Committee comprising of senior executives from the departments of Compliance, Audit &Inspection& International for decision. AGM, KYC & AML Cell-Compliance Department will be the Convener of the Screening Committee. • Reporting of STRs cleared by Screening Committee and approved by Principal Officer to FIU-India. Generation of CCR, CTR, NTR, STR, CBWTR and submission to FIU-IND through Principal Officer. • Maintenance and preservation of records as per the PML Act. • Issuance of Circulars and instructions of RBI's policies and directions to Branches and Zones from time to time and their follow up. • Preparation of tools for KYC compliance including Risk Parameterisation and Categorizing Customer Accounts as per their risk perception. • Evaluation & Monitoring of KYC and AML implementation

	• Implementation of Unique Customer Identification Code (UCIC) & its compliance. • Monitoring & Updation of KYC in KYC non Complied /Frozen Accounts. • Co-ordination of status of KYC and AML implementation through overseeing roles and responsibilities various functional Departments and reporting to various external agencies. • Uploading of KYC documents and data to Central KYC Records Registry.
Inspection Department, Head Office	• Coordinating internal audit/concurrent audit machinery for ensuring adherence to KYC/AML procedures and KYC compliance across all Branches in India. • Issuance of instructions on Risk Categorization of customer accounts to inspectors, concurrent auditors, internal auditors for checking and verification of KYC and AML procedures and commenting on lapses observed thereon.
DIT, Head Office	• To lend technological support for acquisition, establishment and providing Data for CKYCR /AML Solution/Software/Hardware requirement of KYC-AML Cell at Head Office/at other locations. • To examine improvement/modification in acquired software/utilities and up gradation of hardware from its vendors/system integrators from time to time as per requirement. • To develop software including Updation of parameters for generation of alerts for reporting of STR, CTR, CBWTR, NTR statements along with Operations & Services, Audit & Inspection and Compliance Departments. • Continue Updation of software • Checking of accounts of banned entities through Central Server • Periodic Updation of customer risk categorization in the CBS system. • Making provision for recording date of Updation of customer profile in the CBS system • Online verification of PAN number with NSDL • Making provision for capturing details of walk in customers. • Updating periodically the names of banned entity list and checking of existing accounts with banned entity list.
HRM, Head Office	• To plan /schedule/organize adequate on-going training programs / seminars /sessions at Staff College and Training Centers on compliance of KYC-AML-CFT guidelines of the bank with an aim to train maximum number of staff and to co-

	ordinate in this behalf with Audit &Inspection and Compliance Departments. • To provide necessary feedback on number of training programs conducted and number of employees trained, on quarterly basis to Principal Officer. • To arrange training for skill upgradation of staff to observe the behavioral pattern of customers/walk-in customers and reporting of behavioral STR through IRPS menu.
International Department, Head Office	• To cover cross country/Border remittances/Demat/other operations for generation of alerts and to establish suitable mechanism /process/ procedures for verification of such alerts and reporting thereof. • To lay down parameters for approving correspondent Banking relationship. • To oversee the Trade Based Money laundering relating to Export & Import • Monitoring of transactions through SWIFT.
GAD, Head Office	Issue guidelines for maintenance and preservation of records as per the PML Act.

25. Role and Responsibilities of Zonal Head

It has been decided to designate Zonal Heads as Money Laundering Compliance Officer (MLCO) for carrying out bank obligation under PMLA, 2002. Zonal Head to ensure compliance of KYC/AML/CFT norms within the zone:

25.1 Role and Responsibilities of Nodal Officer (ZO*):*

- The Executive designated as Compliance Officer for Compliance Department will act as Nodal Officer for KYC & AML compliance of the Zone.
- Ensure compliance of KYC-AML-CFT Policy/guidelines of the Bank by all the Branches under their control and supervision.
- Ensure timely reporting of SARs and CCRs received from Branches to HO, KYC & AML Cell.
- Consider observations of Internal Inspectors/Concurrent Auditors reported in their Inspection Reports on deficiency or non-compliance of guidelines on KYC-AML-CFT by any of the Branches in the Zone as an Agenda Item in their Review Meeting and ensure rectification thereof by respective Branches.
- Ensure 100% compliance of KYC/AML/CFT guidelines in newly opened accounts and in all existing accounts by their Branches.
- Ensure that the Branches invariably update Customer Identification Data including photo after opening the account once in ten years in case of Low Risk Customers, eight years in case of Medium Risk Customers and once in two years in case of High Risk Customers to meet the Regulatory requirements

- Communication with HO, KYC& AML Cell to ensure smooth implementation of the guidelines especially regarding SARs/STRs/CCRs.

- Dissemination of information to Branches regarding any adverse report circulated in local media/local market for taking cognizance/proper implementation of SAR.

- Training - Ensure holding of training for one/two days seminars /workshops on KYC-AML-CFT guidelines for field functionaries under their jurisdiction once in a year

26. Role and Responsibilities of Branch level:

26.1 Responsibilities of Staff at Branches:

- All the staff members who interact with the customer and/or process/ handle their transactions, whether cash, transfer or clearing, will be responsible for scanning/examination of transactions from money laundering risk perception/angle and bring immediately to the notice of their Branch Head any suspicious transaction/activity of customer observed by them.

- If any time an abnormal behavior / movement of any customer / walk-in-customer / non-customer come to the notice of the Staff member concerned he should bring it to the notice of Branch Head for reporting the same which may be reported as behavioral STR by the Branch, if so deemed fit.

- Any lapse and intentional circumvention on prescribed procedure and guidelines contained in KYC-AML-CFT policy of the bank by any of the staff will be viewed seriously and necessary action as deemed fit will be taken by bank.

- Proper feeding of customer profile i.e. Customer occupation, constitution at the time of creation of new Customer ids and subsequent modification/Updation.

- The particulars KYC documents to be clearly mentioned while updating of customer profile.

- Pan No, Aadhaar number, mobile no. to be invariably checked before verification.

26.2 Responsibilities of Branch Head as KYC & AML Compliance Officer:

- Reporting of Counterfeit Currency (CCRs) to the Zonal Head in the format prescribed (**Annex-16**) within two days from the date of detection/filing FIR for the same. These cash transactions will also include transactions where forgery of valuable security or documents has taken place and will be reported in the form as prescribed by bank to FIU-IND for the present.

- Reporting of Suspicious Activity Report (SAR), behavioral Suspicious Transactions to their Zonal Heads in the physical format prescribed by FIU-IND if any Suspicious Activity is observed by any of the staff members of the Branch.

- Examination/monitoring of High Value Cash Transaction from Money Laundering (ML) angle and reporting of SAR if any from it to their Zonal Heads/HO, KYC& AML Cell through IRPS.
- Monitoring of transaction in accounts for which STRs are reported to FIU-IND.
- Monitoring of transactions in accounts categorized as High/Medium Risk Accounts.
- Ensuring 100% compliance of KYC-AML-CFT policy guidelines of the bank while opening new accounts as well in existing accounts.
- Sending confirmation on quarterly basis to their Zonal Authorities for having complied fully with the KYC-AML-CFT guidelines of the bank in new as well as existing accounts.
- Ensuring Updation of KYC documents (including Photo) of each Low Risk Customer once in ten years from the date of opening account, for medium risk customers once in eight years and for High-Risk Customers once in two years after the date of opening account.
- Ensuring completion of customer profile in all respect for Risk Categorization of new customer while opening the account as well of all the existing customers of the Branch and generating report thereof and preserving the same for inspection by internal inspectors/concurrent Auditors/Reserve Bank of India/ Other Statutory Authorities. [Risk categorization status based on customer profile through AML software is available on IRPS portal-> KYC/AML tab]
- Ensuring review of Risk Categorization as per extant RBI directions/Bank's circular/KYC & AML Policy.
- Not to open accounts recklessly without proper KYC verification and customer Due Diligence.
- Monitoring of transactions in newly opened accounts at least for a period of six months.
- When the signature appears to be changing due to old age or other incapacitation, fresh specimen signature to be obtained and uploaded in the system.
- To create awareness among all staff members regarding risk profile of customers.
- Maintenance of records of prescribed transactions, verification of identity of customers and documents thereof as prescribed in PML ACT, 2002 and mentioned in this policy document.
- Ensuring immediate rectification of deficiencies in KYC Documents if any observed by internal inspectors/Concurrent Auditors/Reserve Bank of India during inspection of the Branch.
- The following reports are submitted by Head Office, AML Cell to FIU-IND.
    1. Cash transactions Report(CTR),
    2. Suspicious activity report (SAR).

3. Suspicious Transaction Report (STR),
4. Counterfeit Currency Report (CCR)
5. Non-government / Non-profit Organizations Transaction Reports (NTR)
6. Cross Border wire transfer report (CBWTR).

- Branches are advised to

1) Download CTRs submitted pertaining to their Branch from IRPS portal-> KYC/AML tab month wise and keep the record available for inspection/audit etc.,
2) Submit behavioral SARs through IRPS portal,
3) Submit the Counterfeit Currency Report (CCR) through Zonal Offices. All the reports to be submitted to their Zonal Office as per guidelines issued from time to time by way of circulars.

The time schedule for submission of the above statements.

No.	Name of the Statement	Date of submission by Branches to Zonal Office	Date of submission by Zonal Office to Head Office
1	Cash Transaction Report (CTR)	Not applicable	Not applicable, since centralized at Head Office.
2	Suspicious Activity Report (SAR)	As and when it is detected by the Branch	As and when it is received from the Branches
3	Counterfeit Currency Report (CCR)	Monthly Consolidated report within 7 days of the subsequent month	Consolidated report within 10 days of the subsequent month
4	NTRs	Not applicable	Not applicable, since centralized at Head Office.
5	CBWTRs	Not applicable	Not applicable, since centralized at Head Office.

26.3 Centralized AML Cell:

Centralized KYC & AML cell has been set up at Head Office under Compliance Department. The cell will look after implementation of KYC/AML/CFT norms in the bank and scrutiny of transactions alerts as mentioned in point no.23.

27. RECORD KEEPING

In terms of the Rule 6, Retention of Records contained in the notification dated 01.07.2005 relating to Prevention of Money Laundering Act issued by the Government of India, the following records shall be maintained / retained for the period prescribed as mentioned in the following paragraphs.

Record (nature and value) of

a) All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

b) All series of cash transactions integrally connected to each other (as explained at end of the sub-head no. (F) which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month;

c) To maintain proper record of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency.

d) 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 has taken place;

e) All suspicious transactions whether or not made in cash and by way as mentioned in the rule :

f) Deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of :

- cheques including third party cheques, pay orders, demand drafts, or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits; or
- traveler cheques; or
- transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts; or
- any other mode in whatsoever name it is referred to :

g) credits or debits into or from any non-monetary accounts such as DEMAT account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be ;

h) Money transfer or remittances in favor of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following :

- payment orders, or
- Cheques, or
- demand drafts, or
- telegraphic or wire transfers or electronic remittances or transfers, or
- internet transfers, or
- Automated Clearing House remittances, or
- any other mode of money transfer by whatsoever name it is called;

i) loans and advances including credit or loan substitutes, investments and contingent liability by way of;

- subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, interbank participation or any other investments in securities or the like in whatever form and name it is referred to, or
- purchase and negotiation of bills, cheques and other instruments, or
- foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or
- letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and / or credit support.
- collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

j) As per Rule 10 of PMLA rules 2005, the identity records of clients shall be maintained for a period prescribed in the following paragraphs.

k) The explanation regarding integrally connected cash transactions referred above is given below. The following transactions have taken place in a month.

Date	**Mode**	**Dr (in Rs.)**	**Cr (in Rs.)**	**Balance (in Rs.) BF - 8,00,000.00**
02.02.2015	Cash	5,00,000.00	3,00,000.00	6,00,000.00
06.02.2015	Cash	40,000.00	2,00,000.00	7,60,000.00
07.02.2015	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly summation		**10,10,000.00**	**6,00,000.00**	

As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total of cash debits during the calendar month exceeds Rs. 10 lakhs. However, the bank should report only the debit transactions taken place on 02/02& 07/02/2015. The debit transaction dated 06/02/2015 which is less than Rs. 50000/- need not be reported separately by the bank.

All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakh and hence credit transaction dated 02/02, 06/02& 07/02/2015 need not be reported by banks.

28. Information to be preserved

Branches shall maintain the following information in respect of records referred to in Rule 3 of PML Rule 2005:

a) The nature of the transactions;

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

c) The date on which the transaction was conducted; and

d) The parties to the transaction.

29. Preservation of records

Branches are required to maintain the records containing information in respect of transactions referred to in Rule 3 of PML Rule 2005. Branches have to take appropriate steps to evolve a system for proper maintenance and preservation of customer information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further in terms of PML Amendment Act 2012 notified on February 15, 2013,**Branches should maintain customer transaction records for at least five years** from the date of transaction between the Bank and the client, so that all necessary records of transaction, domestic or international, could permit reconstruction of individual transaction (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.

Branches should ensure that records pertaining to the identification of the customer and his 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. The identification records and transaction data should be made available to the competent authorities upon request.

Branches are advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/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 in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for five years as is required under PMLA, 2002.

The following information to be preserved in respect of records referred to in Rule 3 of PML Rule 2005:

a) The nature of the transactions;

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

c) The date on which the transaction was conducted; and the parties to the transaction

29A. Bank shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the **DARPAN Portal** of NITI Aayog. Branches shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

30. Reporting to Financial Intelligence Unit-India (FIU-IND)

In terms of the PMLA Rules 2005, banks are required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency, Counterfeit Currency Report (CCRs), Cross Border Wire Transfer Report(CBTRs) involving of Rs.5.00 Lac within 15thof the next month to which it relates through FIN-net portal to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3.at the following address:

Director, FIU-IND, Financial Intelligence Unit-India, 7th Floor, Jeevan Bharti, Building, Tower-II, Connaught Place, Sansad Mard, New Delhi-110001.
Website - http://fiuindia.gov.in/

Branches shall not put any restriction on operations in the accounts merely on the basis of the STR filed. Branches shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information of any transactions and activities which appear unusual, if any such analysis has been done.

31. RECOGNISING AND REPORTING SUSPICIOUS TRANSACTION/ ACTIVITY

31.1 Due Diligence for processing Suspicious Transaction Alerts (STRs) generated through AML software

Suspicious Transaction Alerts (STRs) are generated through AML software centrally on the basis of different threshold put against Alert indicators approved by Indian Bank Association (IBA).The alerts are generated on post transaction basis and it is generated a day after the date of transactions. They are sorted Zone wise and processed/scrutinised by designated Money Laundering Reporting Officer at Head Office.

The PMLA Rule 3(1) (D) read with rule 8 requires the reporting of all suspicious transactions whether or not made in cash. RBI circular dated February 15, 2006 requires that the Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, is 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 Branches/Zones or any other office.

The Grounds of suspicion (GOS) has to be accurate and complete. The grounds of suspicion should express fully 'why' the transaction or activity is unusual, unjustified, does not have economic rationale, or bonafide purpose keeping in mind the banking business and services offered by the Bank. The GOS could also explain the relationship between persons (natural & legal), accounts and transactions that are being reported as part of the STR. Correct reason for suspicion needs to be identified as it signifies the character of suspicious activity/transaction.

GOS need to be in form of a detailed paragraph justifying why the transactions are considered to be suspicious. Specific reference requires to be drawn to the customers' profile, apparent financial standing, past transactions history/activities in account, rationale/purpose behind the transactions, business profile and general transaction pattern etc. These grounds are indicative in nature and may vary from case to case.

At the time of Processing of alerts under STR the Money Laundering Reporting officer (MLRO) should invariably look into the following before taking decision whether the particular alert is to be treated as suspicious or genuine.

(a) Is there any reasonable ground of suspicion that it may involve the proceeds of crime?

(b) The transactions appear to be made in circumstances of unusual or unjustified complexity?

(c) The transactions appear to have no economic rationale or bonafide purpose?

(d) Whether there is reasonable ground of suspicion that it may involve financing of the activities relating to terrorism?

In case if any additional information/Due Diligence is required to be obtained about the customer/transactions; the same may be done through respective Branch.

The designated MLRO after carrying out analysis of the alert, if arrive at a conclusion that the transaction is in tune with the profile of the customer and does not appear to be suspicious may close the alert by recording his/her observations. It is important that MLROs keep proper record of their observations on the closure of alerts which will be useful in case if any regulatory investigations take place in the account at a future date.

If the transactions are not in tune with the profile of the customer and doesn't match with the transactions in normal course, the alerts should be marked as "Suspicious". While marking the alert as "Suspicious", the designated MLRO should furnish the details of "Grounds of Suspicion".

Head office AML cell will further scrutinise such marked alerts in details and submit the findings before the AML Screening Committee with due recommendation either to remove or to report to FIU-IND for their decision.

The maker and checker concept for processing of alerts is introduced and to be followed at all levels.

The records relating to processing & escalation of MLROs to be retained in the system. The records of alerts reported to FIU-IND will be maintained in hardcopies.

Illustrative grounds of suspicion (GOS) are furnished in **Annex-17** and case studies of suspicious activities/transactions are furnished in **Annex-18**.

31.2 Recognizing suspicious transaction / activity

Rules under the PMLA define a "suspicious transaction" as a 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 the proceeds of crime; or (b) appears to be made in circumstances of unusual or unjustified complexity; or (c) appears to have no economic rationale or bonafide purpose (d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Suspicion is personal and subjective and falls far short of proof based on firm evidence. Suspicion may be defined as being beyond mere speculation and based on some foundation i.e. "a degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not", and "although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."

Transaction includes 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.

It is likely that in some cases transactions are abandoned/aborted by customers, on being asked to give details or to provide documents. In that case Branches should report all such attempted transactions in STRs, Even if not completed by customers, irrespective of the amount of the transaction.

"Reasonable grounds to suspect" introduces an objective test rather than the subjective test of suspicion. Thus, it is defined in terms of willful blindness, i.e., turning a blind eye to the obvious; or negligence, i.e., willfully and recklessly failing to make the adequate enquiries that an honest person would be expected to make in the circumstances; or failing to assess adequately the facts and information that are either presented or available and that would put an honest person on enquiry. As such, the staff members must be able to demonstrate that they took all reasonable steps as a person acting in good faith would take in the particular circumstances to know the customer and the rationale for the transaction or the instruction.

31.3 Basis for recognizing suspicions

Satisfactory KYC procedures provide the basis for recognizing unusual and suspicious transactions. The key to recognizing suspicions is knowing enough about the customer and the customer's normal expected activities to recognize when a transaction or an instruction, or a series of transactions or instructions, is / are abnormal.

An illustration of the type of the situations that might give rise to reasonable ground for suspicion in certain circumstances is given below:

- Customer Behavior Indicators
- Transactions which have no apparent purpose and which make no obvious economic sense.
- Where the transaction being requested by the customer without reasonable explanation, is not in line with the services normally requested or is outside the experience of the Bank in relation to the particular customer.

- Where the customer refuses to provide the information requested without reasonable explanation.
- Where a customer, who has entered into a business relationship, uses the relationship for a single transaction or for only a very short period of time.
- The extensive use of offshore accounts, companies or structures in circumstances where the customer's needs do not support such economic requirements.
- Unnecessary routing of funds through third party accounts.
- Unusual investment transactions without apparently discernible profit motive
- An indicative list (not exhaustive) of suspicious activities is also given as **Annex-19.**

31.4 Suspicious Activity Report(SAR)

In order to check possible abuse of banking channel for money laundering / illegal and anti-national activities, the Branches should act as under.

On the basis of information gathered from a prospective customer at the time of filling the relevant Account Opening Form, he / she / the entity be placed under high, medium and low risk category as per the risk classification. However, the customer should not know the category of risk in which he / she / the entity has been placed by the Branch.

- During the currency of an account, the transactions be monitored on regular basis *vis-à-vis* the profile of the customer. Transactions that do not fit in the customer's transaction profile be reviewed by the Departmental In charge.
- In case of transaction carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. Further if Branch has reason to believe that a customer is intentionally structuring a transaction in a series of transactions below the threshold or Rs. 50,000/- the Branch should verify identity and address of the customer and also consider filing a suspicious Activity report (SAR) through IRPS.
- An important element to the success of the AML process is that the customer or the third party is not to be informed (i.e. tipped off)that his / her accounts are under monitoring for suspicious activities and / or that a disclosure has been made to the designated authority. Hence, it should be noted that even after reporting an account or transaction as suspicious, operations are not to be stopped / frozen in such an account. Further, the customer concerned should not come to know that the transaction being suspicious in nature has been reported to the designated authority so as to ensure that no tipping off takes place. Amended sub-rule (3) of Rule 8 of PML Act now requires that banks /financial institutions and its employees should keep the fact of furnishing suspicious activity/transaction information strictly confidential.
- At the same time, all the Branch officials should note that the courteous approach in the process is very essential to take care that the customers are not driven away from the Bank.

- **Screening Mechanism** - SARs/STRs received from Branch (es)/Zonal Office(s) are scrutinized by MLROs at Head Office, AML Cell and placed before the Screening Committee for decision. Thereafter, the same will be placed before the Principal Officer for his comments and subsequent reporting to FIU-IND.

31.5 CASH TRANSACTIONS REPORT - (CTR)

Since all the Branches are under CBS, CTR is generated through AML software centrally at Head Office, for onward transmission to FIU-IND. The reporting shall cover

(a) All cash transactions of Rs.10 lakh and above or its equivalent in foreign currency,

(b) All series of cash transactions integrally connected to each other which have been valued rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh on Monthly basis.

A Copy of monthly CTR generated is made available by DIT to Branches through IRPS for their scrutiny, producing to Auditors/Inspectors when asked for.

While filing CTR, details of individual transactions below Rupees fifty thousand need not be furnished in case of integrally connected transactions mentioned at 24.5.1 (a) above.

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 and should be properly filled up as per instructions given in the instructions part of the related formats of CTR.

Branch should ensure that the instructions on "maintenance of records of transactions", "information to be preserved" and "maintenance and preservation of records" as per the PML Act are scrupulously followed.

31.6 Non Profit Organizations Report (NPOR / NTR):

Non-Profit Organization (NPO) means any entity or organization that is registered as a trust or a society under the Society Registration Act, 1860 or any similar state legislation or a company registered u/s 8 of the Companies Act, 2013.

(a) Government of India vide its Notification No. 13/2009/F.No.6/8/2009-ES dated November, 12 2009 has introduced the above Report.

(b) Reserve Bank of India has directed that the banks / financial institutions are required to Maintain proper record of all transactions involving receipts by non –profit organizations of value more than rupees ten lacs or its equivalent in foreign currency and to forward a report to FIU-IND(Ref: RBI Circular No. DBOD.AML.BC.No.68/14.01.001/2009-10 dated January 12, 2010.

Non-profit organization- Receipts by NPOs of value more than Rs 10 lakh or its equivalent in foreign currency should be submitted every month to Director, FIU-IND by 15th of the succeeding month.

31.7 Counterfeit Currency Report (CCR)

Branches are requested to be guided by Head Office Circular No.CHO/OSD-CC/04/2023-24 dated 11.04.2023 regarding detailed procedure to be followed in case of detection and impounding of counterfeit Notes in line with RBI guidelines RBI/2023-24/98 DCM (FNVD)/G-1/16.01.05/2023-24 dated 03.04.2023.

Whenever a counterfeit note is detected in the cash received by the bank Branch across the counter, it shall be impounded in the presence of the tenderer, in the manner detailed in HO circular mentioned above. For cases of detection of counterfeit notes up to 4 pieces, in a single transaction, a consolidated report should be sent to the police authorities or the Nodal Police Station, along with the suspect counterfeit notes, at the end of the month. For cases of detection of counterfeit notes of 5 or more pieces, in a single transaction, the counterfeit notes should be forwarded immediately to the local police authorities or the Nodal Police Station for investigation by filing FIR. [Formats available in the above mentioned circular]

Acknowledgement of the police authorities concerned has to be obtained for note/s forwarded to them both as consolidated monthly statement and FIR. A proper follow-up of receipt of acknowledgement from the police authorities is necessary. In no case, the counterfeit notes should be returned to the tenderer or destroyed by the bank Branches.

- The Branch/currency chest concerned will prepare the CCR report complete in all respect as per the specified format **(Annex-16)** to currency chest Deptt, GAD, Head Office and Second copy is to be sent to Zonal Office under which the Branch/chest is functioning and the third copy is to be retained by the Branch/chest.

- Zonal Offices on receipt of CCRs from the Branches/currency chest are to compile the position of detection of counterfeit currency note in the zone on a monthly basis and report the same to Currency Chest Department, &Head Office, KYC & AML Cell as per **Annex-16**within 10 days. In case no CCR is received during the month from the Branches/chests, a "NIL" reports is to be sent by ZO to H.O.KYC & AML Cell.

- One CCR should be submitted for each incidence of detection of Counterfeit Indian Currency Note.

- Counterfeit Notes detected at RBI by CVPS machine during processing of soiled notes remitted by currency chest are to be reported by that chest only. At Branch level a FIR should be filed whenever counterfeit notes are detected five or more in number in a single transaction.

- All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the principal officer to FIU-IND immediately in the prescribed format. 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. In view of the above, Branches are advised to maintain proper record of all such 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 transactions and submit the CCR for onward submission to FIU-IND.

Submission of the above report may be prepared manually by the Branches/zonal offices till the Electronic Format is being devised by our IT Department.

31.8 Cross Border Wire Transfer Report (CBWTR)

All cross border wire transfers (CBWTR) of the value of more than rupees Five Lakhs or its equivalent in foreign currency where either the origin or destination of fund is in India; to be reported to FIU-IND. These revised guidelines on reporting of cross border wire transfers (CWTR) have been issued in terms of Circular No. DBOD.AML.NO.16415/14.01.001/2013-14 dated March28, 2014.

32. Prohibition on dealing in Virtual Currencies (VCs).

Virtual currency is a digital representation of value that can be digitally traded andfunctionsas(1)amediumofexchange;and/or(2)aunitofaccount;and/or(3)a storeofvalue,butdoesnothavelegaltenderstatus(i.e.,whentenderedto a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency.

The guidelines on "Prohibition on dealing in Virtual Currencies (VCs)" has been set aside by the Hon"ble Supreme Court.

33. Customer Due Diligence for transactions in Virtual Currencies (VC)

Branches may continue to carry out Customer Due Diligence processes for transactions in Virtual Currencies (VC), in line with the regulations governing standards for Know Your Customer (KYC), Anti-Money laundering (AML), Combating of Financing of Terrorism (CFT) and obligations of regulated entities under Prevention of Money Laundering Act, PMLA.

34. CUSTOMER EDUCATION

For the successful implementation of KYC / AML measures, it is imperative that the Branches should continue their efforts in educating the customers so that they are able to understand the objectives and importance of KYC / AML norms and provide the required information to the Bank while opening accounts without any hassle and, thereafter, conducting operation therein. Literature/pamphlets etc. on the KYC/AML guidelines be given to the customers so as to educate them about the objectives of the KYC Program. The front desk staff should be made fully aware of the KYC/AML guidelines for dealing with the customers. The Bank has distributed to Branches a customer education pamphlet for ready reference on KYC/AML obligations.

35. Employees' Training

Bank has already put in place ongoing employee training programs so that the members of the staff are adequately trained in KYC procedures. The training should take care of the needs of frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently. The staff should be made aware of the precautions they are to adopt and what will be the consequences to the Bank for failure in adhering to KYC and AML norms. Classroom training, videos and technology based training programs can all be used to have good effect

depending on the infrastructure available and the number of people to be trained. All the training Programs of the Bank may include a small training module on KYC/AML procedures, monitoring & reporting including a condensed training programs at entry level for newly recruited officers / clerks. Specialized training program/Workshop shall be conducted once in a year for the Nodal officers (ZO) & MLROs.

36. 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. Therefore, the functional department has to take necessary steps and put adequate screening mechanism while conducting recruitment/hiring process of personnel.

37. PROPER IMPLEMENTATION OF THE POLICY

These guidelines are issued under Section 36(1) (A) of the Banking Regulation Act, 1949 and any contravention of or non-compliance with the same may attract penalties under the relevant provisions of the Act. For legal purposes, the provision contained in the PMLA and rules there under, and instructions issued by RBI from time to time would be applicable.

38. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

Banks shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government.

Branches shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

Further, run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

In case of match in the above cases, Banks shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005.

A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Banks shall file an STR with FIUIND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms, Director, FIU-India has been designated as the CNO.

Banks may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of

Section 12A of the WMD Act, 2005, Banks shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

In case an order to freeze assets under Section 12A is received by the Banks from the CNO, Banks shall, without delay, take necessary action to comply with the Order.

If the process of unfreezing of funds, etc., shall be observed, accordingly the copy of application received from an individual/entity regarding unfreezing shall be forwarded by Bank along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

The latest version of the UNSC Sanctions lists on DPRK is accessible on the UN Security Council's website at the following URLs:

https://www.un.org/securitycouncil/sanctions/1718/materials

to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

Annex–1

Customer KYC/ Due Diligence Procedure: Features to be verified and documents that may be obtained from customers

Customer type	Documents to be obtained for CDD/KYC
Individuals	i. PAN or Form-60 as defined in Income Tax rules, 1962 as amended from time to time. ii. One recent Photograph iii. A certified copy of any OVD containing details of identity & address iv. such other documents pertaining to the nature of business or financial status as decided by the branch. Few such documents are listed hereunder: • Utility bill which is not more than two months old of any service provider (Electricity, Telephone, Postpaid Mobile phone, Piped gas, Water bill) • Property or Municipal tax receipt • Pension or family pension payment order(PPOs) issued to retired employees by Government Departments or Public Sector undertakings, if they contain the address • Letter of allotment of Accommodation from employer issued by Central Govt. departments, Statutory Regulatory Bodies, PSUs, SCBs, FIs & listed companies. Similarly Leave &License agreements with such employers allotting official accommodation. • The customer shall submit OVD with current address within a period of three months of submitting the documents specified above, if address is not updated in OVD's. **A document shall be deemed to be an "Officially valid documents" 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 a Gazette notification, indicating such change of name. [Ref: RBI notification No. DBR.AML.BC.No.46/14.01.001/2015-16 dated 29.10.2015]**
Individuals (NRI and PIO) as defined in FEMA	Original Certified Copy of OVD certified by any one of the following may be obtained • Authorised official of overseas Branches of Scheduled Commercial Bank registered in India

NRI - Non Resident Indian **PIO – Persons of Indian Origin**	• Branches of overseas bank with whom Indian Banks have relationship • Notary Public abroad • Court Magistrate • Judge • Indian Embassy/Consulate General in the country where the non-resident customer resides • 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.
Accounts of companies	i) Certificate of Incorporation ii) Memorandum and Articles of Association iii) PAN of the Company iv) A Resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; v) KYC documents applicable for individuals of all the Authorized Signatories including PAN/Form No.60 to be obtained. vi) KYC documents Relating to Beneficial Ownerthe managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf. vii) The names of the relevant persons holding senior management position; and viii) The address of the registered office and the principal place of its business, if it is different.
Accounts of Registered partnership firms	i) Registration certificate; ii) Partnership deed; and iii) PAN of the Partnership Firm iv) KYC documents applicable for individuals of the person holding an attorney to transact on its behalf. v) KYC documents relating to Beneficial Owner the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf vi) The names of all the partners. vii) The address of the registered office and the principal place of its business, if it is different.

Accounts of trust & foundations	i) Registration Certificate; ii) Trust Deed; and iii) PAN of the Trust iv) Power of Attorney granted to transact on its behalf v) KYC documents applicable for individuals of the person holding an attorney to transact on its behalf. vi) KYC documents relating to Beneficial Owner the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. vii) The name of the beneficiaries, trustees, settler and authors of the trust. viii) The address of the registered office of the trust.
Accounts of Unincorporated association or body of individuals (includes Unregistered Trust, Partnership Firm, Societies.)	i) Resolution of the managing body of such association or body of individuals; ii) Power of Attorney granted to him to transact on its behalf; iii) PAN iv) KYC documents applicable for individuals of the person holding an attorney to transact on its behalf. v) Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals vi) KYC documents relating to Beneficial Owner the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
Accounts of Proprietorship concerns	1. OVDs including PAN/FORM No.60 in respect of the proprietor containing identity and address to be obtained. 2. In addition to the above, any two of the following documents as a proof of business activity in the name of proprietary firm shall also be obtained: i) Registration certificate (in the case of a registered concern) ii) Certificate/License issued by the Municipal Authorities under Shop & Establishment Act iii) Sales and Income tax returns iv) CST/ VAT/GST certificate**(Provisional/Final)** v) Certificate/Registration document issued by Sales Tax/Service Tax/Professional Tax Authorities vi) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/License/certificate of practice issued in the name of the proprietary

	concern by any professional body in corporate under a statute. vii) 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. viii) Utility bills such as electricity, water and landline telephone bills.
Accounts of Self Help Groups(SHG)	i) KYC verification of all the members of self-help groups (SHGs) is not required while opening the savings bank accounts of the SHG. ii) KYC verification of only the officials of the SHGs would suffice. iii) Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs. (As per RBI Circular (RBI/2021-22/10DOR.AML.BC.No.1/14.01.001/2021-22 dated 01st April 2021) iv) KYC documents relating to Beneficial Owner the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
Accounts of Juridical persons such as Govt. or its Departments, Societies, Universities, and Local Bodies like Village Panchayat etc	Certified copy of the following documents to be obtained: i) Document showing name of the person authorized to act on behalf of the entity. ii) PAN/Officially Valid Documents(OVDs) for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf iii) Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person and (DBR.AML.BC.No.18/14/.01.001/2016-17 dated 08.12.2016)

List of Officially Valid Documents (OVD)

1. **Passport**
2. **Voter's Identity Card issued by the Election Commission of India**
3. **Driving License**
4. **Job card issued by NREGA duly signed by an officer of the State Government**
5. **Letter issued by the National Population Register containing details of name and address**
6. **Proof of possession of Aadhaar Number**

Annex- I (A)
Digital KYC Process

A. The Bank 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 Bank.

B. The access of the Application shall be controlled by the Bank 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 Bank to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Branch or vice-versa. The original OVD shall be in possession of the customer.

D. The Bank 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 Bank shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Bank) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the Bank 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 Bank shall not be used for customer signature. The Bank 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 Bank. 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 Bank, 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 Branch/Bank 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 Bank/Branch, 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.

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

The procedure for identification of Beneficial Owner as advised by the Government of India is as under. Rule 9(3) Amendments of PML 2013

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 a controlling ownership interest or who exercises control through other means.

Explanation.- For the purpose of this sub clause:

(i) "Controlling ownership interest" means ownership of or entitlement to more than 10 %(ten percent)of shares or capital or profits of the company;

(ii) "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 ownership of/entitlement to majority more than 10 % (ten percent) 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 ownership of or entitlement to more than 15% (fifteen percent) of the property or capital or profits of such association or body of individuals (societies).

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

e) 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 10 % (ten percent) 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;

Branches to be guided by Bank's Circular CHO/COMP/KYC&AML/2021/83 dated 01/07/2020 in this regard.

Annex - 3

Date :.....

To,

Branch Manager

UCO Bank

.....Branch

Dear Sir,

Re: My Deposit Account No.....

Today, I have opened the above deposit account with your Bank with the reduced KYC procedure since I intend to keep balances not exceeding Rs. 50,000/- in all my accounts taken together with the Bank and that total credit in all the accounts taken together would not exceed Rs. 1 lakh in a year. I am aware that if at any point of time, the balances in all my accounts with the Bank taken together exceed Rs. 50,000/- or total credit in all the accounts exceeds Rs.1 lakh in a year, the Bank shall be within its rights to stop further transactions in the accounts until full KYC procedure is completed by me. Details of my other accounts, if any, with your Bank are as under:

Nature of account with account number	**Branch of UCO BANK where kept**

Yours faithfully,

Signature of Depositor

Name……..……..

Address ……

Annex - 4

UCO BANK

.....Branch

Shri / Ms .....

Dear Sir / Madam,

Re: Your Deposit Account No(s) .....with us

1. Your above mentioned account(s) was / were opened by applying reduced KYC procedure since you intended to keep balance not exceeding Rs. 50,000/- in all your accounts taken together with the Bank and total credit in all the accounts taken together not exceeding Rs. 1 lakh in a year.

2 We have to inform that balance in your above account(s) taken together have reached / crossed Rs. 40,000/- and / or the total credit in a year has reached / crossed Rs. 80,000/-. As such, please visit our Branch at the earliest along with the following documents so that full KYC procedure, as per the directives of the Reserve Bank of India, could be conducted :

(a)

(b)

(c)

3 Please note that in the event of non-submission of the above mentioned documents within a period of we shall be constrained to freeze all your accounts when the balance exceeds Rs. 50,000/- or total credit exceeds Rs. 1 lakh in a year, at your risk and responsibility.

Thanking you,

Yours faithfully,

Date :

Branch Head

Annex - 5

Certificate of verification of the address of the account holder

The undersigned visited the premises
at

.....

.....(Address to be given) and, on enquiry, it is revealed that Shri/Ms.....who has opened / submitted papers for opening Saving Bank A/c / Current Account No

.....

.....on..... (date of opening / submission of papers for opening the account) is residing at the above-mentioned address for the last …….. Years / months.

Signature

.....

Name of the

Employee

.....

Designation..

Date:

Action taken by the Deposit Department

DELETED

Annex– 6

SPECIMEN OF LETTER OF INTRODUCTION TO BE OBTAINED ON BANK'S LETTER HEAD

Ref No…… Date:……

Telephone No……FAX No……

The Manager

UCO Bank

……

Re: Introductory letter for opening of current account for……(mention purpose)

We hereby introduce the account of Messrs .....having current account no .....with us since.....The firm is availing following credit facilities from our Bank:

Sl No.	Nature of facility	Amount (Rs. In Lakh)

- It is the proprietary / partnership / private limited / limited company with the following constitution:

  (a) (b) (c) (d)
- The following are the authorized signatories in the account:

Name	Address	Designation of signatories

- We confirm / verify / attest the signatures / photographs of the signatories. Photographs of each signatory are attached.
- The loan accounts of the party with us are running satisfactorily and we have no objection for opening of current account of the party with your Branch for the purpose of availing duty drawback/other facility (Specify).
- Any other information

Thanking You.Faithfully,

Manager / Senior Manager (with bank stamp / seal)

Annex-7(a)

Indicative Alert Indicators for Branches/ Departments

S. No.	Alert Indicator	Indicative Rule / Scenario
1	CV1.1 - Customer left without opening account	• Customer did not open account after being informed about KYC requirements
2	CV2.1 - Customer offered false or forged identification documents	• Customer gives false identification documents or documents that appears to be counterfeited, altered or inaccurate
3	CV2.2 - Identity documents are not verifiable	• Identity documents presented are not verifiable i.e. Foreign documents etc.
4	CV3.1 - Address found to be non-existent	• Address provided by the customer is found to be non-existent
5	CV3.2 - Address found to be wrong	• Customer not staying at address provided during account opening
6	CV4.1 - Difficult to identify beneficial owner	• Customer uses complex legal structures or where it is difficult to identify the beneficial owner
7	LQ1.1 - Customer is being investigated for criminal offences	• Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences
8	LQ2.1 - Customer is being investigated for TF offences	• Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities
9	MR1.1 - Adverse media report about criminal activities of customer	• Match of customer details with persons reported in local media / open source for criminal offences
10	MR2.1 - Adverse media report about TF or terrorist activities of customer	• Match of customer details with persons reported in local media / open source for terrorism or terrorist financing related activities
11	EI1.1 - Customer did not complete transaction	• Customer did not complete transaction after queries such source of funds etc.
12	EI2.1 - Customer is nervous	• Customer is hurried or nervous
13	EI2.2 - Customer is over cautious	• Customer over cautious in explaining genuineness of the transaction.
14	EI2.3 - Customer provides inconsistent information	• Customer changes the information provided after more detailed information is requested. • Customer provides information that seems minimal, possibly false or inconsistent.

S. No.	Alert Indicator	Indicative Rule / Scenario
15	EI3.1 - Customer acting on behalf of a third party	• Customer has vague knowledge about amount of money involved in the transaction. • Customer taking instructions for conducting transactions • Customer is accompanied by unrelated individuals.
16	EI3.2 - Multiple customers working as a group	• Multiple customers arrive together but pretend to ignore each other
17	EI4.1 - Customer avoiding nearer Branches	• Customer travels unexplained distances to conduct transactions
18	EI4.2 - Customer offers different identifications on different occasions	• Customer offers different identifications on different occasions with an apparent attempt to avoid linkage of multiple transactions.
19	EI4.3 - Customer wants to avoid reporting	• Customer makes inquiries or tries to convince staff to avoid reporting.
20	EI4.4 - Customer could not explain source of funds	• Customer could not explain source of funds satisfactorily
21	EI5.1 - Transaction is unnecessarily complex	• Transaction is unnecessarily complex for its stated purpose.
22	EI5.2 - Transaction has no economic rationale	• The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer.
23	EI5.3 - Transaction inconsistent with business	• Transaction involving movement of which is inconsistent with the customer's business
24	EI6.1 – Unapproved inward remittance in NPO	• Foreign remittance received by NPO not approved by FCRA
25	PC1.1 - Complaint received from public	• Complaint received from public for abuse of account for committing fraud etc.
26	BA1.1 - Alert raised by agent	• Alert raised by agents about suspicion
27	BA1.2 - Alert raised by other institution	• Alert raised by other institutions, subsidiaries or business associates including cross-border referral

Annex-7(b)

Indicative Alert Indicators for Centralized AML Cell

S. No.	Alert Indicator	Indicative Rule / Scenario
1	WL1.1 - Match with UN list	• Match of customer details with individuals/ entities on various UNSCR Lists
2	WL1.2 - Match with UAPA List	• Match of customer details with designated individuals/entities under UAPA
3	WL1.3 - Match with other TF list	• Match of customer details with TF suspects on lists of Interpol, EU, OFAC, Commercial lists (World-Check, Factiva, LexisNexis, Dun & Bradstreet etc.) and other sources
4	WL2.1 - Match with other criminal list	• Match of customer details with criminals on lists of Interpol, EU, OFAC, Commercial lists (World-Check, Factiva, LexisNexis, Dun & Bradstreet etc.) and other sources
5	TM2.1 - High value cash deposits in a month	• Cash deposits greater than INR [X1] for individuals and greater than INR [X2] for non-individuals in a month • Top [N] cash deposits in a month
6	TM2.2 - High value cash withdrawals in a month	• Cash withdrawals greater than INR [X1] for individuals and greater than INR [X2] for non-individuals in a month • Top [N] cash withdrawals in a month
7	TM2.3 - High value non-cash deposits in a month	• Non-Cash deposits greater than INR [X1] for individuals and greater than INR [X2] for non-individuals in a month • Top [N] non-cash deposits in a month
8	TM2.4 - High value non-cash withdrawals in a month	• Non-Cash withdrawals greater than INR [X1] for individuals and greater than INR [X2] for non-individuals in a month • Top [N] non-cash withdrawals in a month
9	TM3.1 - Sudden high value transaction for the client	• Value of transaction is more than [Z] percent of the previous largest transaction for the client (or client profile)
10	TM3.2 - Sudden increase in value of transactions in a month for the client	• Value of transactions in a month is more than [Z] percent of the average value for the client (or client profile)
11	TM3.3 - Sudden increase in number of transactions in a month for the client	• Number of transactions in a month is more than [Z] percent of the average number for the client (or client profile)
12	TM4.1 - High value transactions in a new account	• Transactions greater than INR [X] in newly opened account within [Y] months
13	TM4.2 - High activity in a new account	• Number of transactions more than [N] in newly opened account within [Y] months
14	TM5.1 - High value transactions in a dormant account	• Transactions greater than INR [X] in dormant account within [Y] days of reactivation

S. No.	Alert Indicator	Indicative Rule / Scenario
15	TM5.2 - Sudden activity in a dormant account	• Number of transactions more than [N] in dormant account within [Y] days of reactivation
16	TM6.1 - High value cash transactions inconsistent with profile	• Cash transactions greater than INR[X] by customer with low cash requirements such as Students, Housewife, Pensioners, Wages and salary Person and Minor Accounts
17	TM6.2 - High cash activity inconsistent with profile	• Number of cash transactions greater than [X] by customer with low cash requirements such as Students, Housewife, Pensioners, Wages and salary Person and Minor Accounts
18	TY1.1 - Splitting of cash deposits just below INR 10,00,000 in multiple accounts in a month	• Cash deposits in amounts ranging between INR 9,00,000/- to INR 9,99,999.99) in multiple accounts of the customer greater than [N] times in a month
19	TY1.2 - Splitting of cash deposits just below INR 50,000	• Deposit of cash in the account in amounts ranging between INR 40,000/- to INR 49,999/- greater than [N] times in [Y] days
20	TY1.5 - Frequent low cash deposits	• Cash deposits in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days
21	TY1.6 - Frequent low cash withdrawals	• Cash withdrawals in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days
22	TY2.1 - Many to one fund transfer	• Funds sent by more than [N] remitters to one recipient
23	TY2.2 - One to many fund transfer	• Funds sent by one remitter to by more than [N] recipients
24	TY3.1 - Customer providing different details to avoid linkage	• Customer provided different IDs or Date of Birth at different instances
25	TY3.2 - Multiple customers working together	• Common address/telephone used by multiple unrelated customers • Common IDs used by multiple customers • Group of individuals conducting transactions at the same time
26	TY5.1 - Majority of repayments in cash	• Card repayments greater than INR [X] amount in cash in [Y] days • Card repayment in cash is greater than [Z] percent of repayments in [Y] days
27	TY5.2 - Large debit balance in credit card	• Debit balance in credit card is greater than INR[X]
28	TY5.3 - Large value card transactions for purchase of high value goods	• Card usage greater than INR [X] for jewellery (MCC 5944) in [Y] days

S. No.	Alert Indicator	Indicative Rule / Scenario
29	TY5.4 - Large value cash withdrawals against international card	• Cash withdrawals greater than INR [X] against international card in [Y] days
30	TY5.5 - Repeated small value cash withdrawals against international card	• Cash withdrawals against international card in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days in locations with known terrorist incidents
31	TY5.6 - Large repetitive card usage at the same merchant	• More than [N] transactions at same merchant aggregating to more than INR [X] in [Y] days
32	TY7.1 - Repayment of loan in cash	• Loan repayments in cash greater than INR [X] in [Y] months
33	TY7.2 - Premature closure of large FDR through PO/DD	• Premature closure of FDR for amount greater than INR [X] within [N] days and payment by PO/DD
34	TY7.3 - High number of cheque leaves	• Greater than [X1] number cheque leaves issued for savings bank account and [X2] number of cheque leaves issued for Current account in a period of [Y] days
35	TY7.4 - Frequent locker operations	• Number of locker operations greater than [X] times in [Y] days
36	RM1.1 - High value transactions by high risk customers	• Transactions greater than INR [X] by high risk customers
37	RM1.2 - High value cash transactions in NPO	• Cash transactions greater than INR [X] in Trust/NGO/NPO in [Y] days
38	RM1.3 - High value cash transactions related to real estate	• Cash transactions greater than INR [X] related to real estate transactions in [Y] days
39	RM1.4 - High value cash transactions by dealer in precious metal or stone	• Cash transactions greater than INR [X] by dealer in precious metal, precious stone or high value goods in [Y] days
40	RM2.2 - High value inward remittance	• Inward remittance greater than [X] value aggregated in [Y] days
41	RM2.3 - Inward remittance in a new account	• Inward remittance greater than [X] value in a new account within [Y] days
42	RM2.4 - Inward remittance inconsistent with client profile	• Inward remittance greater than [X] value in [Y] days in account of Students, Housewife, Pensioners, Wages and salary Person and Minor Accounts
43	RM3.1 - High value transactions with a country with high ML risk	• Transaction greater than INR [X] involving a country considered to be high risk from the money laundering or drug trafficking perspective.

Annex-7(C)

Red Flag on Trade based Money Laundering (TBML)

S. No.	RFI No.	Red Flag Indicator	Proposed Manner of Implementation
1	1	Inward remittance followed by immediate withdrawal/transfer to other accounts.	To be considered while conducting Due Diligence under automated transaction monitoring.
2	2	Wash sales or round trip sales - Accounts debited and then immediately credited or vice versa for related purchase/sale.	To be considered while conducting Due Diligence under automated transaction monitoring.
3	3	Client is involved in high risk or cash intensive business such as money remitting.	To be considered while conducting Due Diligence under automated transaction monitoring.
4	4	Sudden increase in cash deposits of clients involved in high risk business.	To be considered while conducting Due Diligence under automated transaction monitoring.
5	5	Use of multiple accounts by customer; or accounts operated for very short period and used for advance remittances only.	To be considered while conducting Due Diligence under automated transaction monitoring/review.
6	6	Little or no withdrawal from account for business purposes/ no recurrent business expenses.	To be considered while conducting Due Diligence under automated transaction monitoring.
7	7	Multiple cash deposits in one country followed by immediate ATM withdrawal in another country.	To be considered while conducting Due Diligence under automated transaction monitoring.
8	9	Funds received but goods not exported - advance for exports.	Through quarterly statement of overdue export advances submitted to RBI.
9	10	Funds sent out but goods not imported – advance for imports.	Scrutiny of BEF for transactions above USD 100,000; Internal reports to be developed for transaction less than USD 100,000.
10	14	Consignment size is unreasonable compared to	Consignment size/transaction value to be considered for inclusion in transaction

S. No.	RFI No.	Red Flag Indicator	Proposed Manner of Implementation
		customer profile/capacity/size of business.	checklist, compared to customers' profile and track record. Additional Due Diligence can be performed as part of the Due Diligence under normal transaction monitoring procedures.
11	16	Underlying goods or services not in line with customer's profile and declared business.	To be implemented through operational checklist for customer or transaction Due Diligence for higher value transactions (for single transaction or on aggregate basis).
12	18	Transactions related to acquisition or sale of intangibles like PIN, e-codes, specialized software, etc.	To be included as part of the document checklist and transaction Due Diligence in line with FEMA provisions.
13	21	Transactions involving third parties which may not be contract parties (consignee and remitter are different).	To be included as part of the document checklist and transaction Due Diligence in line with FEMA provisions.
14	27	Description of goods provided is vague.	To be included as part of the document checklist and transaction Due Diligence.
15	28	Prima facie the documents submitted look suspicious.	To be included as part of the document checklist.
16	29	Substantial inconsistencies between the information originally supplied and that contained in the documents.	To be included as part of the document checklist. In case of LCs, if discrepancies are accepted, the Bank may accept this as a waiver of discrepancies and pay.
17	30	Suspected discrepancies between description of goods on transport document vis-à-vis invoice/other documents.	To be included as part of the document checklist.
18	34	Import payments being made against old bills after lapse of considerable period of time from import of goods, without appropriate justification and documentation.	To be included as part of the document checklist and transaction Due Diligence and as mandated by RBI guidelines on import of goods & services.

S. No.	RFI No.	Red Flag Indicator	Proposed Manner of Implementation
19	35	Remittances to or from high risk jurisdictions.	This RFI is part of the transaction monitoring scenario already in place. Can be included as part of the document checklist.
20	36	Goods transshipped through high risk jurisdictions for no apparent reason.	To be implemented through document checklist.
21	38	Amounts of money transfer carried out by natural persons and legal entities are multiples of 100/1,000/10,000/100,000 USD/EUR/National currency.	To be implemented through normal transaction Due Diligence procedures.
22	41	Structuring of transactions to avoid threshold reporting.	To be monitored through alert based transaction monitoring procedures RFI to be made part of the Due Diligence procedures.
23	42	Structuring of transactions to avoid submission of BOE (Remittance amounts kept just below the threshold of USD 100,000 or equivalent value).	To be monitored through alert based transaction monitoring procedures RFI to be made part of the Due Diligence procedures.
24	44	Originator/beneficiary information missing in wire transfers.	To be checked as part of transaction Due Diligence for compliance with wire transfer guidelines.
25	46	Use of repeatedly amended or frequently extended letters of credit without reasonable justification or for reasons like changes of beneficiary or location.	RFI to be made part of the document checklist.
26	47	Accounts funded by negotiable instruments (such as travelers' cheques, cashier's cheques, etc.) in round denominations.	To be considered while conducting Due Diligence.
27	48	Importer of goods not from the same country from where wire (payment for import) originated.	Third Party Import guidelines as per RBI guideline to be followed.

S. No.	RFI No.	Red Flag Indicator	Proposed Manner of Implementation
28	50	Packing inconsistent with the commodity or shipping method.	To be included as part of document checklist; documents to be checked for consistency between invoice, packing list, shipping bills, etc.
29	58	A customer deviates significantly from its historical pattern of trade activity (i.e. in terms of markets, monetary value, and frequency of transactions, volume, or merchandise type).	To be implemented through transaction monitoring and document checklists.
30	59	Transacting parties appear to be affiliated, conduct business out of a residential address, or provide only a registered agent's address.	This RFI can be implemented for high value transactions, as it is very difficult for the banks to determine affiliated parties based on available information in the usual course.
31	60	The LC contains non-standard clauses or phrases or has unusual characteristics.	To be made part of the document checklist.

RFIs agreed to be implemented (modifications)

S. No.	RFI No.	Red Flag Indicator	Proposed Manner of Implementation
1	8	Monitor activity in newly opened accounts for initial 6 months'.	To be considered while conducting Due Diligence under automated transaction monitoring.
2	20	Due Diligence for high seas sales/ merchanting trades'.	Transaction Due Diligence to be conducted in line with FEMA provisions for high seas sales/ merchanting trades.
3	22	Inward remittances made through exchange houses.'	To be monitored through transaction checklist or other manual procedures.
4	40	'Customer not able to provide/ justify rationale for source of funds.'	To be monitored as part of the transaction and normal alert Due Diligence. The RFI to be implemented on a risk based approach.
5	43	Receipt of multiple payments via internet payment service provider like Paypal, etc.'	To be considered as part of the transaction monitoring Due Diligence.

S. No.	RFI No.	Red Flag Indicator	Proposed Manner of Implementation
6	53	'High value remittances for frequent ticket/tour packages booked by tour operators'.	To be considered as part of the checklist during transaction monitoring Due Diligence.
7	55	Forex for medical treatment as per prescribed limit but availed multiple times by the same individual in a year'.	To be considered as part of the transaction monitoring Due Diligence.

S. No.	RFI No.	Red Flag Indicator	Proposed Manner of Implementation
1	11	Advance for supply of goods is a major part/percentage of the total value of goods.	To be implemented on a best effort basis.
2	12	Amount of advance is not in line with normal international trade for the kind of goods.	To be implemented on a best effort basis.
3	17	Transaction not in-line with normal international trade for the given kind of goods & parties involved.	To be implemented on a best effort basis.
4	26	Trade activity done from port which is far from the importer/exporter's base location. Example importer is in Surat and goods imported through a remote port in Assam.	To be implemented on a best effort basis.
5	31	Unnecessarily complex transactions that lack economic sense.	To be implemented on a best effort basis.
6	49	Foreign based importing entity with accounts in exporting country receiving payments from locations outside the area of it's customer base.	For better clarity, RFI to be modified to 'Routing of import payments through India by a foreign based entity having operations and customer base outside India'. To be implemented on a best effort basis.

~~Annex-8~~

~~DELETED~~

Certificate for the quarter ended _____

Name of Zone: **Date:**_____

A.

Sl No.	**Particulars**	**Position as of previous quarter ended…….**	**Position as of last quarter ended……..**
1.	Number of Customers		
2.	Number of KYC complied Customers		
3.	Number of KYC non-complied Customers		
4.	Number of a/cs frozen due to KYC non compliance		

B. Steps taken for 100% KYC compliance in the system

_____

_____

We certify that all the Branches are complying with KYC & AML norms.

(Signature of Dy. Zonal Head) (Signature of Zonal Head)

Annex-9

Indicative list of High Risk countries

1. Democratic Republic of Korea
2. Iran
3. Myanmar
4. Albania
5. Barbados
6. Bulgaria
7. Burkina Faso
8. Cameroon
9. Cayman Islands
10. Democratic Republic of Congo
11. Croatia
12. Gibraltar
13. Haiti
14. Jamaica
15. Jordan
16. Mali
17. Mozambique
18. Nigeria
19. Philippines
20. Senegal
21. South Africa
22. South Sudan
23. Syria
24. Tanzania
25. Turkey
26. Uganda
27. United Arab Emirates
28. Vietnam
29. Yemen

Annex-10

High Net worth Individuals

Customer Type/Constitution	High Risk Annual Income	Medium Risk Annual Income	Low Risk Annual Income
Individuals	Above Rs.25.00 Lac	Above Rs.10.00 Lac &Up to Rs.25.00 Lac	Up to Rs. 10.00 Lac
Clubs & Associations	Above Rs.25.00 Lac	Above Rs.10.00 Lac &Up to Rs.25 Lac	Up to Rs.10 .00 Lac
Sole Proprietorship firms	Above Rs.1.00 Crore	Above Rs.50.00 Lac &Up to 1.00 Crore	Up to Rs. 50.00 Lac
Partnership Firms	Above Rs.5.00 Crore	Above Rs.1.00 Crore to 5.00 Crore	Up to Rs. 1.00 Crore
Limited Cos Public/Private	Above Rs.25.00 Crore	Above Rs.5.00 crore&up to Rs. 25.00 Crore	Up to Rs. 5.00 Crore

Annex 11

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

North Block, New Delhi.
Dated: the 2nd February, 2021

ORDER

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

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) 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.

2. In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure is outlined below in supersession of earlier orders and guidelines on the subject:

3. Appointment and communication details of the UAPA Nodal Officers:

3.1 The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA **[Telephone Number: 011-23092548, 011-23092551 (Fax), email address: jsctcr-mha@gov.in].**

3.2 The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

3.4 All the States and UTs shall 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 Central [designated] Nodal Officer for the UAPA.

3.5 The Central [designated] Nodal Officer for the UAPA shall maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers, in July every year or as and when the list is updated and shall cause the amended list of UAPA Nodal Officers circulated to all the Nodal Officers.

3.6 The Financial Regulators shall forward the consolidated list of UAPA Nodal Officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies.

3.7 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the consolidated list of UAPA Nodal Officers to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs.

4. Communication of the list of designated individuals/entities:

4.1 The Ministry of External Affairs shall update the list of individuals and entities subject to the UN sanction measures whenever changes are made in the lists by the UNSC 1267 Committee pertaining to Al Qaida and Da'esh and the UNSC 1988 Committee pertaining to Taliban. On such revisions, the Ministry of External Affairs would electronically forward the changes without delay to the designated Nodal Officers in the Ministry of Corporate Affairs, CBIC, Financial Regulators, FIU–IND, CTCR Division and Foreigners Division in MHA.

4.2 The Financial Regulators shall forward the list of designated persons as mentioned in Para 4(i) above, without delay to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies.

4.3 The Central [designated] Nodal Officer for the UAPA shall forward the designated list as mentioned in Para 4(i) above, to all the UAPA Nodal Officers of States/UTs without delay.

4.4 The UAPA Nodal Officer in Foreigners Division of MHA shall forward the designated list as mentioned in Para 4(i) above, to the immigration authorities and security agencies without delay.

4.5 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the list of designated persons as mentioned in Para 4(i) above, to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs without delay.

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

5.1 The Financial Regulators will issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by the SEBI and insurance companies requiring them -

(i) To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, 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, 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, insurance companies shall immediately 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 Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email 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 5.1 (ii) above to the UAPA Nodal Officer of the State/UT where the account is held and to Regulators and FIU-IND, as the case may be, without delay.

(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 shall prevent such designated persons from conducting financial transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Fax No.011-23092551 and also convey over telephone No.011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in, without delay.

(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 under Paragraph 5.1(ii) above, carried through or attempted as per the prescribed format.

5.2 On receipt of the particulars, as referred to in Paragraph 5 (i) above, the Central [designated] Nodal Officer for the UAPA 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 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 expeditiously from the date of receipt of such particulars.

5.3 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 orders to freeze these assets under Section 51A of the UAPA would be issued by the Central [designated] nodal officer for the UAPA without delay and conveyed electronically to the concerned bank branch, depository and insurance company under intimation to respective Regulators and FIU-IND. The Central [designated] nodal officer for the UAPA shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and all UAPA nodal officers in the country, 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 Central [designated]

Nodal Officer for the UAPA 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.

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

6.1 The Central [designated] Nodal Officer for the UAPA shall electronically forward the designated list to the UAPA Nodal Officers of all States and UTs with 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, without delay.

6.2 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 Central [designated] Nodal Officer for the UAPA without delay at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post would necessarily be conveyed on email id: jsctcr-mha@gov.in.

6.3 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 shall be completed without delay and shall be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to the Central [designated] Nodal Officer for the UAPA at the given Fax, telephone numbers and also on the email id.

6.4 The Central [designated] Nodal Officer for the UAPA may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

6.5 In case, the results of the verification indicates that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA shall be issued by the Central [designated] Nodal Officer for the UAPA without delay 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.

6.6 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 becoming aware of any transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

7. Regarding the real-estate agents, dealers of precious metals/stones (DPMS) and other Designated Non-Financial Businesses and Professions (DNFBPs) and any other person:

(i) The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned Regulators without delay.

(a) The DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transactions and, without delay, inform the UAPA Nodal officer of the State/UT with details of the funds/assets held and the details of the transaction, who in turn would follow the same procedure as in para 6.2 to 6.6 above. Further, if the dealers hold any assets or funds of the designated individual/entity, either directly or indirectly, they shall freeze the same without delay and inform the UAPA Nodal officer of the State/UT.

(ii) The CBIC shall advise the dealers of precious metals/stones (DPMS) that if any designated individual/entity approaches them for sale/purchase of precious metals/stones or attempts to undertake such transactions the dealer should not carry out such transaction and without delay inform the CBIC, who in turn follow the similar procedure as laid down in the paragraphs 6.2 to 6.5 above.

(iii) The UAPA Nodal Officer of the State/UT shall advise the Registrar of Societies/ Firms/ non-profit organizations that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar should inform the UAPA Nodal Officer of the State/UT without delay, who will, in turn, follow the procedure as laid down in the paragraphs 6.2 to 6.5 above. The Registrar should also be advised that no societies/ firms/ non-profit organizations should be allowed to be registered, if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and in case such request is received, then the Registrar shall inform the UAPA Nodal Officer of the concerned State/UT without delay, who will, in turn, follow the procedure laid down in the paragraphs 6.2 to 6.5 above.

(iv) The UAPA Nodal Officer of the State/UT shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino and/ or if any assets of such designated individual/ entity is with the Casino operator, and of the particulars of any client matches with the particulars of designated individuals/ entities, the Casino owner shall inform the UAPA Nodal Officer of the State/UT without delay, who shall in turn follow the procedure laid down in paragraph 6.2 to 6.5 above.

(v) The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI) requesting them to sensitize their respective members to the provisions of Section 51A of UAPA, so that if any

designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of Designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(vi) The members of these institutes should also be sensitized that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any of designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(vii) In addition, the member of the ICSI be sensitized that if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person then the member should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(viii) The Registrar of Companies (ROC) may be advised that in case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with ROC or beneficial owner of such company, then the ROC should convey the complete details of such designated individual/ entity, as per the procedure mentioned in paragraph 8 to 10 above. This procedure shall also be followed in case of any designated individual/ entity being a partner of Limited Liabilities Partnership Firms registered with ROC or beneficial owner of such firms. Further the ROC may be advised that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm and in case such a request received the ROC should inform the UAPA Nodal Officer in the Ministry of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(ix) Any person, either directly or indirectly, holding any funds or other assets of designated individuals or entities, shall, without delay and without prior notice, cause to freeze any transaction in relation to such funds or assets, by immediately informing the nearest Police Station, which shall, in turn, inform the concerned UAPA Nodal Officer of the State/UT along with the details of the funds/assets held. The concerned UAPA Nodal Officer of the State/UT, would follow the same procedure as in para 6.2 to 6.6 above.

8. Regarding implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001:

8.1 The U.N. Security Council Resolution No.1373 of 2001 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.

8.2 To give effect to the requests of foreign countries under the 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 Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.

8.3 The Central [designated] Nodal Officer for the UAPA shall cause the request to be examined without delay, 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.

9. Upon receipt of the requests by these Nodal Officers from the Central [designated] Nodal Officer for the UAPA, the similar procedure as enumerated at paragraphs 5 and 6 above shall be followed.

The freezing orders shall be issued without prior notice to the designated persons involved.

10. Regarding exemption, to be granted to the above orders in accordance with UNSCR 1452.

10.1 The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the Central [designated] nodal officer of the UAPA to be:-

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

(b) necessary for extraordinary expenses, provided that such determination has been notified by the MEA;

10.2. The addition may be allowed to accounts of the designated individuals/ entities subject to the provisions of paragraph 10 of:

(a) interest or other earnings due on those accounts, or

(b) payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of resolutions 1267 (1999), 1333 (2000), or 1390 (2002),

Provided that any such interest, other earnings and payments continue to be subject to those provisions;

11. Regarding 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:

11.1 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, ROC, Regulators of DNFBPs and the UAPA Nodal Officers of State/UT.

11.2 The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs 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 Central [designated] Nodal Officer for the UAPA as per the contact details given in Paragraph 3.1 above, within two working days.

11.3 The Central [designated] Nodal Officer for the UAPA shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, he/she shall pass an order, without delay, 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, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officer of State/UT. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Central [designated] Nodal Officer for the UAPA shall inform the applicant expeditiously.

12. Regarding prevention of entry into or transit through India:

12.1 As regards prevention of entry into or transit through India of the designated individuals, the UAPA Nodal Officer in 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.

12.2 The immigration authorities shall ensure strict compliance of the order and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the UAPA Nodal Officer in Foreigners Division of MHA.

13. Procedure for communication of compliance of action taken under Section 51A: The Central [designated] Nodal Officer for the UAPA and the Nodal Officer in the Foreigners Division, 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.

14. Communication of the Order issued under Section 51A of Unlawful Activities (Prevention) Act, 1967: The order issued under Section 51A of the Unlawful Activities (Prevention) Act, 1967 by the Central [designated] Nodal Officer for the UAPA relating to funds, financial assets or economic resources or related services, shall be communicated to all the UAPA nodal officers in the country, the Regulators of Financial Services, FIU-IND and DNFBPs, banks, depositories/stock exchanges, intermediaries regulated by SEBI, Registrars performing the work of registering immovable properties through the UAPA Nodal Officer of the State/UT.

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

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

To,

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) Secretary, Ministry of Corporate Affairs, New Delhi

8) Chairman, Central Board of Indirect Taxes & Customs, New Delhi.

9) Director, Intelligence Bureau, New Delhi.

10) Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.

11) Chief Secretaries of all States/Union Territories

12) Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories

13) Directors General of Police of all States & Union Territories

14) Director General of Police, National Investigation Agency, New Delhi.

15) Commissioner of Police, Delhi.

16) Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.

17) Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance, New Delhi.

18) Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.

19) Director (FIU-IND), New Delhi.

Copy for information to: -

1. Sr. PPS to HS

2. PS to SS (IS)

Annex- 12

Anti-Money Laundering Questionnaire

Name of the Financial Institutions:……

Location:

……..

Anti-Money Laundering Questionnaire			
I.	**General AML Policies, Practices and Procedures :**		
1.	Does the AML compliance program require approval of the FI's Board or a senior committee thereof?	**Y**	**N**
2.	Does the FI have a legal and regulatory compliance program that includes a designated Compliance officer that is responsible for coordinating and overseeing the AML program on a day-to-day basis, which has been approved by senior management of the FI?		
3	Has the FI developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions that has been approved by senior management?		
4	In addition to inspections by the government supervisors/regulators, does the FI client have an internal audit function or other Independent third party that assesses AML policies and practices on a regular basis?		
5	Does the FI have a policy prohibiting accounts / relationships with shell banks (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated to a regulated financial group)?		
6	Does the FI have policies covering relationships with politically exposed persons consistent with industry best practices?		
7	Does the FI have appropriate record retention procedures pursuant to applicable law?		
8	Does the FI require that its AML policies and practices be applied to all Branches and subsidiaries of the FI both in the home country and in locations outside of the home country?		
II.	***Risk Assessment***		
9	Does the FI have a risk focused assessment of its customer base and transactions of its customers?		

10	Does the FI determine the appropriate level of enhanced Due Diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?		
III. Know Your Customer, Due Diligence and Enhanced Due Diligence			
11	Has the FI implemented systems for the identification of its customers, including customer information in the case of recorded transactions, account opening, etc. (for example; name, nationality, street address, telephone number, occupation, age/date of birth, number and type of valid official identification, as well as the name of the country/state that issued it)?		
12	Does the FI have a requirement to collect information regarding its customers' business activities?		
13	Does the FI collect information and assess its FI customers' AML policies or practices?		
14	Does the FI have procedures to establish a record for each customer noting their respective identification documents and Know Your Customer Information collected at account opening?		
15	Does the FI take steps to understand the normal and expected transactions of its customers based on its risk assessment of its customers?		
IV.	***Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds***		
16.	Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?		
17.	Does the FI have procedures to identify transactions structured to avoid large cash reporting requirements?		
18.	Does the FI screen transactions for customers or transactions the F1 deems to be of significantly high risk (which may include persons, entities or countries that are contained on lists issued by government/international bodies) that special attention to such customers or transactions is necessary prior to completing any such transactions?		
19.	Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has		

	no physical presence and which is unaffiliated to a regulated financial group.)		
20.	Does the FI have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?		
	V. ***Transaction Monitoring***		
21	Does the FI have a monitoring program for suspicious or unusual activity that covers funds transfers and monetary instruments (such as travellers cheques, money orders, etc.)?		
	VI. **AML Training**		
22	Does the FI provide AML training to relevant employees that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?		
23	Does the FI retain records of its training sessions including attendance records and relevant training materials used?		
24	Does the FI have policies to communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?		
25	Does the FI employ agents to carry out some of the functions of the FI and if so does the FI provide AML training to relevant agents that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?		

Financial Institution Name:
Location:
Name:
Title:
Signature:
Date:

Annex-13

Categorization of Foreign Investors

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 Portfolio Investment Scheme (PIS) route not eligible under Category I and II above such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

Annex-14

KYC documents Requirement for 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	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 of Bank accounts etc. is not in vogue, may submit 'Power of Attorney granted to Global Custodian/Local Custodian in lieu of Board Resolution'

Annex-15

The prevention of Money Laundering Act, 2002 and the Rules notified there under impose various obligations on banking companies, financial institutions and intermediaries.

Obligations of Reporting Entities under PMLA

Obligations	**When**
Communicate the name , designation and address of the Principal Officer to FIU-IND.	At the time of appointment / change of Principal Officer.
Verify identity, current address including permanent address, nature of business and financial status of the client.	At the time of opening an account or executing any transaction.
Formulate and implement a Client Identification Programme (CIP) to determine true identity of clients and forward a copy of the same to FIU-IND	At the time of formulation/modification of CIP.
Evolve internal mechanism for maintaining and furnishing information.	Ongoing
Furnish Cash Transaction Report (CTR) to FIU-IND containing specified cash transactions.	Within 15th day of succeeding month (Monthly Reporting).
Furnish Non-Profit Organization Transaction Report (NTR) to FIU-IND.	Within 15th day of succeeding month (Monthly Reporting).
Furnish Cross Border Wire transfer Report (CBWTR) to FIU-IND.	Within 15th day of succeeding month (Monthly Reporting).
Furnish Counterfeit Currency Report (CCR) to FIU-IND.	Within 15th day of succeeding month.
Furnish Suspicious Transaction Report (STR) to FIU-IND containing details of all suspicious transactions whether or	Within 7 working days on being satisfied that the transaction is suspicious.

not made in cash, including attempted suspicious transactions.	
Maintain records of identity of clients.	For a period of 5 years after cessation of relationship with the client.
Maintain records of all transactions reported to FIU-IND.	For a period of 5 years after the date of transaction.

Annex-16

Format for reporting Counterfeit Currency Report (CCR)

Name of the Branch/Currency Chest/Zonal Office _____

Counterfeit Currency Report (CCR) dated from _____to _____

The consolidated Report must be reached to Compliance-KYC & AML Cell, Head Office before 7th day of the subsequent month of detection as "Fake Note" by Fax- 033 44559425 or Email-gmop.calcutta@ucobank.co.in

Sl. No.	Name of Branch/ Currency Chest	SOL Id.	Branch Details	Details of Fake Currency Notes detected						
				Date of Cash Tendering	Date of Detection	Total Amount Deposited	Value of Fake Note	No. of Fake Notes	Currency Serial	Remark If Any
1	2	3	4	5	6	7	8	9	10	11
	Total									

Summary of Counterfeit Currency Note:- (Summary of format above)

Sl No.	Denomination	No. of Pieces		Value in Rs.
1	2000			
2	1000			
3	500			
4	200			
5	100			
6	50			
7	20			
8	10			
	Total			

Name
Designation

Name

Designation

Encl: Annexure-I (FIR details, if any)

Annex- 17

Illustrative grounds of suspicion (GOS)

Banking Companies

No.	Suspicion	Summary of detection and review
1	False Identity	Identification documents were found to be forged during customer verification process. The account holder was not traceable
2	Wrong Address	Welcome pack was received back as the person was not staying at the given address or address details given by the account holder were found to be false. The account holder was not traceable
3	Doubt over the real beneficiary of the account	The customer not aware of transactions in the account. Transactions were inconsistent with customer's profile.
4	Account of persons under investigation	The customer was reported in media for being under investigation.
5	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth / Father's name / Nationality) were same as a person on the watch list of UN, Interpol etc.
6	Account used for cyber crime	Complaints of cyber crime were received against a customer. No valid explanation for the transactions by account holder.
7	Account used for lottery fraud	Complaints were received against a bank account used for receiving money from the victims. Deposits at multiple locations followed by immediate cash withdrawals using ATMs. No valid explanation provided by the account holder.
8	Doubtful activity of a customer from high risk country	Cash deposited in a bank account at different cities on the same day. The account holder a citizen of a high risk country with known cases of drug trafficking.
9	Doubtful investment in IPO	Large number of accounts involving common introducer or authorized signatory. Accounts used for multiple investments in IPOs of various companies.
10	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter-account transactions without any economic rationale.
11	Unexplained activity in dormant accounts	Sudden spurt in activity of dormant account. The customer could not provide satisfactory explanation for the transactions.
12	Unexplained activity in account inconsistent with the declared business	Transactions in account inconsistent with what would be expected from declared business. The customer could not provide satisfactory explanation.

13	Unexplained large value transactions inconsistent with client's apparent financial standing	Large value transactions in an account which usually has small value transactions. No valid explanation provided by the account holder.
14	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known sources of income.
15	Suspicious use of ATM card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
16	Doubtful use of safe deposit locker	Safe deposit locker operated frequently though the financial status of client
17	Doubtful source of cash deposited in bank account	Frequent cash transactions of value just under the reporting threshold. Cash transactions split across accounts to avoid reporting. No valid explanation provided.
18	Suspicious cash withdrawals from bank account	Large value cheques deposited followed by immediate cash withdrawals.
19	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.
20	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list.
21	Doubtful beneficiary of foreign remittances	Name and other details of the beneficiary matches with a person on watch list.
22	Doubtful utilizations of foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation.
23	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organizations.

Financial Institutions:

No.	Suspicion	Summary of detection and review
24	Doubtful source of insurance	• Substantial premium paid by cash/demand draft in premium multiple insurance policies without valid explanation. • Substantial premium paid by multiple demand

		drafts of amounts below Rs.50,000. • Insurance premium much beyond declared sources of income.
25	Doubtful source of loan foreclosure	Substantial amount paid in cash / demand draft for foreclosure of loan account. No valid explanation provided.
26	Doubtful source of the inward foreign remittances	Inward foreign remittance received from a non relative. No valid explanation provided by the beneficiary.
27	Suspicious inward foreign remittances	Splitting of inward foreign remittances to collect funds in cash in an apparent attempt to avoid fund trail.
28	Doubtful beneficiary of foreign remittances	Doubtful credentials of the beneficiary. No valid explanation for the remittance provided.
29	Doubtful purchase of foreign exchange by a customer	Substantial foreign exchange purchased in cash or demand draft. No valid explanation provided.

Intermediaries

No.	Suspicion	Summary of detection and review
31	Doubtful source of investment in mutual funds	Substantial investment in multiple folios in short span. Form 60/61 provided for substantial investment. No valid explanation provided.
32	Doubtful ownership of investment in mutual funds	Large investment in mutual fund using third party cheques. No valid explanation provided.
33	Suspicious off market transactions in demat accounts	Off-market transfer of shares from multiple demat accounts to one demat account. No valid explanation provided. Suspected share price manipulation by bulk off-market transactions.

Annex-18

Case Studies of Suspicious Activities

Case Study 1

Mercury Leather Impex Pvt Ltd. deals in manufacture and export of rexin goods, as per the documents provided. Transactions in the account were normal with no inward or outward remittances. Customer receives an inward remittance of INR 5.5m and issues cheques for smaller amounts to various persons. Customer explains the transaction as proceeds of an export of wrist watches to Dubai. No proof shown regarding trading in wrist watches and no explanation given for the pay outs. Unusual transaction and Activity not in line with the known business/ source of funds - an apt case for raising a SAR.

Key Message

Continuously look out for transactions not in line with the customer's known business activity.

Case Study 2

RD Group, a well known group in city KK has non-borrowal relationship with the bank. Operated three main accounts, one a private limited co. and two partnership firms.Mr. RD is MD in the pvt.ltd. co. and partner in others. Around 15 other accounts of the group where about 10 persons, believed to be employees of the group, operated the accounts as proprietors or partners in various combinations. Large cash deposits and very frequent inter-account transfers. I.T. made enquiries about operations in some of the accounts. During verification, it was found that addresses in some of the accounts were non-existent. Group explained that they sell of goods to retailers and that generate cash and they are also in real estate business. Multiple accounts are maintained for efficient tax management. Since the transactions lacked transparency and verifications were negative, decided to exit relationship. Some of the existing accounts in the group were not KYC compliant. It was known to the staff in KK that all the 15 odd accounts were being operated as a group. They should have questioned the necessity of all these accounts and the transactions going through these accounts. SARs should have been raised, if proper explanation was not forthcoming on the transactions.

Key Message

Do not compromise compliance for revenue. Apply caution in case of regular inter group transfers with no apparent economic sense.

Case Study 3

Money Transfers

The police arrested suspect A, the leader of an Iranian drug trafficking group, for possessing stimulants and other kinds of drugs. The subsequent investigation revealed that the suspect had remitted part of his illegal proceeds abroad. A total of US$450,000 was remitted via three banks to an account on behalf of suspect as

older brother B at the head office of an international bank in Dubai. Transfers were made on five occasions during a two-month period in amounts ranging from US$50,000 to US$150,000. Another individual, suspect C, actually remitted the funds and later returned to Iran. On each occasion C took the funds in cash to the bank, exchanged them for dollars, and then had the funds transferred. Each of the transactions took about one hour to conduct, and the stated purpose for the remittances was to cover "living expenses". Suspect A was initially charged with violating provisions of the anti-narcotics trafficking law. The money transfers revealed during the investigation led to additional charges under the anti-money laundering law.

Key Message

This case represents a classic example of a simple money laundering scheme and is also a good example of a case derived, not just from suspicious transaction reporting, but also as a follow-up to traditional investigative activity.

Case Study 4

Launderers recruit individuals for the use of their bank account.

An FIU received suspicious transaction reports from three financial institutions concerning international fund transfers. Through police investigation, it was discovered that several individuals were acting as money collectors for a cocaine trafficking organisation. The job of these individuals was to identify and "recruit" professionals already established in various trades and services who might be amenable to earning some extra money by allowing their bank accounts to be used in a laundering scheme. The professionals would place cash in their accounts and then transfer the sum to accounts indicated by the money collectors.

The professionals who became involved in this activity were active in several types of business, including travel agencies, and import/export in commodities and computers. In return for their services, they received a commission on the funds transferred through their accounts. The transfers out of the accounts were justified by fictitious invoicing that corresponded to their particular business.

This investigation uncovered an organisation that was laundering the proceeds of cocaine trafficking believed to be worth US$ 30 million. Several members of the group were identified and tried in two countries.

Key Message

This scheme illustrates how criminals put additional measures into place further to distance the money from the narcotics trafficking operation. Cash is collected from the drug dealer; the collector passes the funds to the launderer; the launderer then passes them to the recruited business professional, who then transfers the funds abroad for further processing. The money continues to move, and the trail becomes more complex. The use of professionals can establish a 'break' in the trail, and so thwart financial investigators.

Case Study 5

Use of bank safety deposit boxes

A law enforcement investigation centred on the suspicious behaviour of a bank customer who appeared to be exchanging old, outdated banknotes for a new series of banknotes. The suspect appeared to be storing the old banknotes in one of the bank's safety deposit boxes.

The suspect received social security payments and had no other identifiable legitimate income.

Further enquiries revealed that the suspect had an extensive criminal history and had recently purchased a motor vehicle with a large amount of cash and owned a number of high value real estate properties.

The investigation established that the suspect was involved in drug cultivation in the houses that he had purchased using the proceeds of his drug trafficking activities. The suspect was using the bank's safety deposit facilities to store cash obtained from the sale of the illegal drugs and also to store jewellery purchased with the same proceeds.

Key Message

This example illustrates that a complicated money laundering scheme is not always necessary to integrate illegal proceeds back into the circulation. The frequent locker operation to be monitored and any suspicion is to be reported as SAR.

Case Study 6

Payments structured to avoid detection

Over a four year period, Mr. A and his uncle operated a money remittance service known as Company S and conducted their business as an agent of a larger money remitting business that was suspected of being used to finance terrorism. Later, an investigation was initiated in relation to Company S based on a suspicious transaction report.

The investigation showed that over the four year period, Mr. A's business had received over US$4 million in cash from individuals wishing to transmit money to various countries. When Mr. A's business received the cash from customers, it was deposited into multiple accounts at various Branches of banks in country X. In order to avoid reporting requirements in place in Country X, Mr. A and others always deposited the cash with the banks in sums of less than US$10,000, sometimes making multiple deposits of less than US$10,000 in a single day.

Mr. A was charged and pleaded guilty to a conspiracy to "structure" currency transactions in order to evade the financial reporting requirements.

Key Message

This case underlines the need to have mechanisms in place to monitor and link transactions (especially cash deposits) made by the same individual or entity through different Branches of the same bank, or through different banks.

Case Study 7

Silver and gold smuggling

Cross-jurisdictional investigations permitted the detection of a silver and gold smuggling system aimed at VAT evasion and the laundering of the illicit profits of several local, regional and global criminal organisations. The banking and financial systems were used to process large-value transactions supporting the fictitious payment of precious metals supplies. The laundering was primarily undertaken through:

Creation of a network of companies, including financial, throughout the region, with the task of "filtering" the money. Using criminal proceeds derived from cigarette smuggling, drug trafficking, illegal arms trafficking and the smuggling of oil products, to purchase silver and gold, which was in turn smuggled into the markets of Country J and other European countries. Reinvestment of the profits of the illicit trafficking of silver into smuggling activities.Use of false invoices in respect of the importation of precious metals which never actually reached country J. Use of bearer savings deposit passbooks and of false Treasury certificates of deposit to be offered as guarantees to the banks for the purchase of precious metals.

Fifteen suspects were arrested for criminal conspiracy aimed at money laundering and smuggling, and four suspects were charged with money laundering offences. The total amount of funds involved was US$101mn with the consequent evasion of export duties amounting to US$72mn, VAT evasion totalling US$37mn and the laundering of over US$31mn.

Key Message

Enquiries should always be undertaken to ascertain the purpose and beneficial ownership of companies that are formed in offshore jurisdictions with lax corporate registration requirements. The source of the economic activity that created the funds for transfer should be established. Where the sale of precious metals is involved, checks should be made that the goods exist and that excise duty and VAT has been paid.

Case Study – 8

A person X opened a saving account in 2009 in a Bank with a deposit of Rs.500/-. There was no transaction above Rs.10000/- in next two years. In year 2011, all of sudden, Rs.2 lac was deposited by cheque in the account and immediately withdrawal the amount through ATM. The pattern was repetitive in nature. While the matter was investigated, the account holder informed that he/she has not done any such transactions. Later it has come to notice that cheques were stolen and deposited in the account without the knowledge of the a/c holder. Sudden high

value deposit in an account followed by immediate withdrawal of fund triggers suspicion. An opt case of STR.

Key Message

Abnormal transactions in a low turnover account should be monitored.

ANNEX -19

AN INDICATIVE LIST (NOT EXHAUSTIVE) OF SUSPICIOUS ACTIVITIES

Transactions involving large Transactions involving large amounts of cash

(i) Exchanging an unusually large amount of small denomination notes for those of higher denomination.

(ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the Bank.

(iii) Frequent withdrawal of large amounts by means of cheques including traveler's cheques.

(iv) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.

(v) Large cash withdrawals from a previously dormant / inactive account or from an account which has just received an unexpected large credit from abroad.

(vi) Company transactions, both deposits and withdrawals that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, for example, cheques, letters of credit, bills of exchange, etc.

(vii) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

Transactions which do not make economic sense

(i) A customer having a large number of accounts with the Bank with frequent transfers between different accounts.

(ii) Transactions in which assets are withdrawn immediately after being deposited unless the customer's business activities furnish a plausible reason for immediate withdrawal.

Activities not consistent with the customer's business

(i) Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.

(ii) Corporate accounts where deposits and withdrawals by cheque / telegraphic transfers / foreign inward remittances / any other means are received from / made to sources apparently unconnected with the corporate business activity / dealings.

(iii) Unusual applications for DD / TT / PO against cash.

(iv) Accounts with large volume of credits through DD / TT / PO whereas the nature of business does not justify such credits.

(v) Retail deposit of many cheques but rare withdrawals for daily operations.

Attempts to avoid reporting / record-keeping requirements

(i) A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

(ii) Any individual or group of individuals that coerces / induces or attempts to coerce / induce the Bank employee not to file any report or any other form.

(iii) An account where there are several cash deposits / withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual activities

(i) An account of a customer who does not reside / have office near the Branch even though there are bank Branches near his residence / office.

(ii) A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.

(iii) Funds coming from the list of countries / centres which are known for money laundering.

Customer who provides insufficient or suspicious information

(i) A customer / company who is reluctant to provide complete information with regard to the purpose of the business, prior banking relationship, officers or directors, or its locations.

(ii) A customer / company who is reluctant to reveal details about its activities or to provide financial statements.

(iii) A customer who has no record of past or present employment but makes frequent large transactions.

Certain suspicious funds transfer activities

(i) Sending or receiving frequent or large volumes of remittances to / from countries outside India.

(ii) Receiving large TT / DD remittances from various centres and remitting the consolidated amount to a different account / centre on the same day leaving minimum balance in the account.

(vi) Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire / funds transfer

Certain Bank employees arousing suspicion

(i) An employee whose lavish lifestyle cannot be supported by his or her salary.

(ii) Negligence of employees / willful blindness is reported repeatedly.

Examples of suspicious activities / transactions to be monitored by the operating staff

(i) Large cash transactions.

(ii) Multiple accounts under the same name.

(iii) Frequently converting large amount of currency from small to large denomination notes.

(iv) Placing funds in term deposits and using them as security for more loans.

(v) Large deposits immediately followed by wire transfers.

(vi) Sudden surge in activity level.

(vii) Same funds being moved repeatedly among several accounts.

(viii) Multiple deposits of money orders, banker's cheques, drafts of third parties.

(ix) Transactions inconsistent with the purpose of the account.

(x) Maintaining a low or overdrawn balance with high activity.

Check list for preventing money-laundering activities

(i) A customer maintains multiple accounts, transfers money among the accounts and uses one account as a master account from which wire / funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).

(ii) A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering of money.

(iii) A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

(iv) A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.

(v) A customer experiences increased wire activity when previously there has been no regular wire activity.

(vii) Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

(vii) A business customer uses or evidences or sudden increase in wired transfer to send and receive large amounts of money, internationally and / or domestically and such transfers are not consistent with the customer's history.

(viii) Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.

(ix) Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.

(x) Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

(xi) Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.

(xii) Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

(xiii) Periodic wire transfers from a person's account/s to Bank haven countries.

(xiv) A customer pays for a large (international or domestic) wire transfer using multiple monetary instruments drawn on several financial institutions.

(xv) A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques.

(xvi) A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when

- the amount is very large (say over Rs.10 lakh);
- the amount is just under a specified threshold (to be decided by the Bank based on local regulations, if any);
- the funds come from a foreign country; or
- Such transactions occur repeatedly.

(viii) A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold). A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

Annex-20

SUSPICIOUS TRANSACTION REPORT REGISTER

Name of the Customer	
Occupation / Business of the Party	
Nature of account and number	
Date of opening the account	
Amount of suspicious transaction and currency	
Date of transaction	
Annual turnover / income last declared by the account holder	
Details of the transaction	
Reasons for considering the transaction suspicious	
Name and designation of the reporting officer with signature	

Signature (with name) of the reporter .....

Date :.....

Orders of the Branch Head .....

Signature of the Branch Manager with date

(Name……..……..)

Annex -21
F.No.P - 12011/2022-ES Cell-DOR
Government of India
Ministry of Finance
Department of Revenue
****

New Delhi, dated the 30th January, 2023.

ORDER

Subject: - Procedure for implementation of Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005"

Section 12A of The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 [hereinafter referred to as 'the Act'] reads as under: -

"*12A. (1) No person shall finance any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.*

(2) For prevention of financing by any person of any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

a) freeze, seize or attach funds or other financial assets or economic resources—

i. owned or controlled, wholly or jointly, directly or indirectly, by such person; or

ii. held by or on behalf of, or at the direction of, such person; or

iii. derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under this Act, or under the United Nations (Security Council) Act,1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

II In order to ensure expeditious and effective implementation of the provisions of Section 12A of the Act, the procedure is outlined below.

1. Appointment and communication details of Section 12A Nodal Officers:

1.1 In exercise of the powers conferred under Section 7(1) of the Act, the Central Government assigns Director, FIU-India, Department of Revenue, Ministry of Finance, as the authority to exercise powers under Section 12A of the Act. The Director, FIU-India shall be hereby referred to as the Central Nodal Officer (CNO) for the purpose of this order. **[Telephone Number: 011- 23314458, 011- 23314435, 011-23314459 (FAX), email address: dir@fiuindia.gov.in].**

1.2 **Regulator** under this order shall have the same meaning as defined in Rule 2(fa) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. **Reporting Entity (RE)** shall have the same meaning as defined in Section 2 (1) (wa) of Prevention of Money-Laundering Act, 2002. DNFPBs is as defined in section 2(1) (sa) of Prevention of Money-Laundering Act, 2002.

1.3 The Regulators, Ministry of Corporate Affairs and Foreigners Division of MHA shall notify a Nodal Officer for implementation of provisions of Section 12A of the Act. The Regulator may notify the Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act. All the States and UTs shall notify a State Nodal officer for implementation of Section 12A of the Act. A State/UT may notify the State Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act.

1.4 The CNO shall maintain an updated list of all Nodal Officers, and share the updated list with all Nodal Officers periodically. The CNO shall forward the updated list of all Nodal Officers to all REs.

2. Communication of the lists of designated individuals/entities:

2.1 The Ministry of External Affairs will electronically communicate, without delay, the changes made in the list of designated individuals and entities (hereinafter referred to as 'designated list') in line with section 12A (1) to the CNO and Nodal officers.

2.1.1 Further, the CNO shall maintain the Designated list on the portal of FIU-India. The list would be updated by the CNO, as and when it is updated, as per para 2.1 above, without delay. It shall make available for all Nodal officers, the State Nodal Officers, and to the Registrars performing the work of registration of immovable properties, either directly or through State Nodal Officers, without delay.

2.1.2 The Ministry of External Affairs may also share other information relating to prohibition / prevention of financing of prohibited activity under Section 12A (after its initial assessment of the relevant factors in the case) with the CNO and other organizations concerned, for initiating verification and suitable action.

2.1.3 The Regulators shall make available the updated designated list, without delay, to their REs. The REs will maintain the designated list and update it, without delay, whenever changes are made as per para 2.1 above.

2.2 The Nodal Officer for Section 12A in Foreigners Division of MHA shall forward the updated designated list to the immigration authorities and security agencies, without delay.

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

3.1 All Financial Institutions shall –

i. Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of designated list and in case of match, REs shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved *to* the CNO by email, FAX and by post, without delay.

ii. Run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, Insurance policies etc. In case, the particulars of any of their customers match with the particulars of designated list, REs shall immediately 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 on their books *to* the CNO by email, FAX and by post, without delay.

iii. The REs shall also send a copy of the communication, mentioned in 3.1 (i) and (ii) above, *to* State Nodal Officer, where the account/transaction is held, and to their Regulator, as the case may be, without delay.

iv. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A, REs shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post , without delay.

3.2 On receipt of the particulars, as referred to in Paragraph 3.1 above, the CNO 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 REs are the ones in designated list and the funds, financial assets or economic resources or related services, reported by REs are in respect of the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

3.3 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned RE under intimation to respective Regulators. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All Nodal officers in the country, 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. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

3.4 The order shall be issued without prior notice to the designated individual/entity.

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

4.1 The Registrars performing work of registration of immovable properties shall –

i. Verify if the particulars of the entities/individual, party to the transactions, match with the particulars of the designated list, and, in case of match, shall not carry out such transaction and immediately inform the details with full particulars of the assets or economic resources involved *to* the State Nodal Officer, without delay.
ii. Verify from the records in their respective jurisdiction, without delay, on given parameters, if the details match with the details of the individuals and entities in the designated list. 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 Registrar shall immediately inform the details with full particulars of the assets or economic resources involved *to* the State Nodal Officer, without delay.

iii. In case there are reasons to believe beyond doubt that assets that are held by an individual/entity would fall under the purview of clause (a) or (b) of subsection (2) of Section 12A, Registrar shall prevent such individual/entity from conducting transactions, under intimation to the State Nodal Officer by email, FAX and by post , without delay.

4.2 the State Nodal Officer would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources to the CNO without delay by email, FAX and by post.

4.3 The State Nodal Officer may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed, within 24 hours of the verification, if it matches, with the particulars of the designated individual/entity, to the CNO without delay by email, FAX and by post.

4.4 The CNO may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

4.5 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned Registrar performing the work of registering immovable properties, and to FIU under intimation to the concerned State Nodal Officer. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All Nodal officers in the country, 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. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

4.6 The order shall be issued without prior notice to the designated individual/entity.

5. Regarding the real-estate agents, dealers of precious metals/stones (DPMS), Registrar of Societies/ Firms/ non-profit organizations, The Ministry of Corporate Affairs and Designated Non-Financial Businesses and Professions (DNFBPs):

(i) The dealers of precious metals/stones (DPMS) as notified under PML (Maintenance of Records) Rules, 2005 and Real Estate Agents, as notified under clause (vi) of Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002, are required to ensure that if any designated individual/entity approaches them for sale/purchase of precious metals/stones/Real Estate Assets or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12ANodal officer in the Central Board of Indirect Taxes and Customs (CBIC). Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Nodal officer in the CBIC, who will, in turn, follow procedure similar to as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6.

(ii) Registrar of Societies/ Firms/ non-profit organizations are required to ensure that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6 above. The Registrar should also ensure that no societies/ firms/ non-profit organizations should be allowed to be registered if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and, in case, such request is received, then the Registrar shall inform the State Nodal Officer, without delay.

(iii) The State Nodal Officer shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino or if any assets of such designated individual/ entity are with the Casino operator, or if the particulars of any client match with the particulars of designated individuals/ entities, the Casino owner shall inform the State Nodal Officer, without delay, and shall freeze any such transaction.

(iv) The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI), requesting them to sensitize their respective members to the provisions of Section 12A, so that, if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall in turn follow the similar procedure as laid down for State Nodal Officer in paragraph 4.2 to 4.6 above.

(v) The members of these institutes should also be sensitized by the Institute of Chartered Accountants of India, Institute of Cost and Work Accountants of India and Institute of Company Secretaries of India (ICSI) that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete

details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(vi) In addition, a member of the ICSI shall, if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person, convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer, if such company, limited liability firm, partnership firm, society, trust, or association holds funds or assets of the designated individual/entity.

(vii) In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm, and in case such a request is received, the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(viii) All communications to Nodal officer as enunciated in sub clauses (i) to (vii) above should, inter alia, include the details of funds and assets held and the details of transaction.

(ix) The Other DNBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Central Nodal officer. The communication to the Central Nodal Officer would include the details of funds and assets held and the details of the transaction. Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Central Nodal officer.

(DNFBPs shall have the same meaning as the definition in Section 2(1) (sa) of Prevention of Money-Laundering Act,2002.)

5.1. All Natural and legal persons holding any funds or other assets of designated persons and entities, shall, without delay and without prior notice, freeze any transaction in relation to such funds or assets and shall immediately inform the State Nodal officer along with details of the funds/assets held, who in turn would follow the same procedure as in para 4.2 to 4.6 above for State Nodal Officer. This obligation should extend to all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

5.2 No person shall finance any activity related to the 'designated list' referred to in Para 2.1, except in cases where exemption has been granted as per Para 6 of this Order.

5.3. Further, the State Nodal Officer 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 in the designated list. The State Nodal Officer shall, upon becoming aware of any transactions and attempts by third party, without delay, bring the incidence to the notice of the CNO and the DGP/Commissioner of Police of the State/UT for initiating suitable action.

5.4 Where the CNO has reasons to believe that any funds or assets are violative of Section 12A (1) or Section 12A (2)(b) of the Act, he shall, by order, freeze such funds or Assets, without any delay, and make such order available to authorities, Financial Institutions, DNFBPs and other entities concerned.

5.5 The CNO shall also have the power to issue advisories and guidance to all persons, including FIs and DNFBPs obligated to carry out sanctions screening. The concerned Regulators shall take suitable action under their relevant laws, rules or regulations for each violation of sanction screening obligations under section 12A of the WMD Act.

6. Regarding exemption, to be granted to the above orders

6.1. The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the CNO to be: -

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, consequent to notification by the MEA authorizing access to such funds, assets or resources.

This shall be consequent to notification by the MEA to the UNSC or its Committee, of the intention to authorize access to such funds, assets or resources, and in the absence of a negative decision by the UNSC or its Committee within 5 working days of such notification.

(b) necessary for extraordinary expenses, provided that such determination has been notified by the MEA to the UNSC or its Committee, and has been approved by the UNSC or its Committee;

6.2. The accounts of the designated individuals/ entities may be allowed to be credited with:

(a) interest or other earnings due on those accounts, or

(b) payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of section 12A of the Act.

Provided that any such interest, other earnings and payments continue to be subject to those provisions under para 3.3;

6.3 Any freezing action taken related to the designated list under this Order should not prevent a designated individual or entity from making any payment due under a contract entered into prior to the listing of such individual or entity, provided that:

(i) the CNO has determined that the contract is not related to any of the prohibited goods, services, technologies, or activities, under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems;

(ii) the CNO has determined that the payment is not directly or indirectly received by an individual or entity in the designated list under this Order; and

(iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorise, where appropriate, he unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorization.

7. **Regarding 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 individual or entity is not a designated person or no longer meet the criteria for designation:**

7.1 Any individual/entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held has been inadvertently frozen, an application may be moved giving the requisite evidence, in writing, to the relevant RE/Registrar of Immovable Properties/ ROC/Regulators and the State.

7.2 The RE/Registrar of Immovable Properties/ROC/Regulator and the State Nodal Officer shall inform, and forward a copy of the application, together with full details of the asset frozen, as given by applicant to the CNO by email, FAX and by Post, within two working days. Also, listed persons and entities may petition a request for delisting at the Focal Point Mechanism established under UNSC Resolution.

7.3 The CNO shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, it shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer. However, if it is not possible, for any reason, to pass an Order unfreezing the assets within 5 working days, the CNO shall inform the applicant expeditiously.

7.4 The CNO shall, based on de-listing of individual and entity under UN Security Council Resolutions, shall pass an order, if not required to be designated in any other order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer.

8. Procedure for communication of compliance of action taken under Section 12A: The CNO and the Nodal Officer in the Foreigners Division, 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.

9. Communication of the Order issued under Section 12A: The Order issued under Section 12A of the Act by the CNO relating to funds, financial assets or economic resources or related services, shall be communicated to all nodal officers in the country.

10. This order is issued in suppression of F.No.P-12011/14/2022-ES Cell-DOR, dated 30th January 2023.

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

(Manoj Kumar Singh)
Director (HQ)

To,
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) Secretary, Ministry of Corporate Affairs, New Delhi
8) Chairman, Central Board of Indirect Taxes & Customs, New Delhi.
9) Director, Intelligence Bureau, New Delhi.
10) Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
11) Chief Secretaries of all States/Union Territories
12) Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
13) Directors General of Police of all States & Union Territories
14) Director General of Police, National Investigation Agency, New Delhi.
15) Commissioner of Police, Delhi.
16) Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
17) Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance, New Delhi.
18) Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.
19) Director (FIU-IND), New Delhi.

Copy for information to: -
1. Sr. PPS to HS
2. PS to SS (IS)

Annexure-22

(SELF DECLARATION IN CASE OF NO CHANGE IN KYC INFORMATION INCLUDING PAN/Form 60 OF INDIVIDUAL CUSTOMER)

I undertake that there is no change in my KYC information as already submitted to the bank for

Name of Account Holder……

Account/Customer ID Number…… (Need not to submit separately for multiple accounts, ID is must in multiple accounts)

Contact/Mobile Number:……

I also undertake that I have already submitted PAN No…… /Form 60 (whichever is not applicable to be strike off)

(Signature of account holder)

In case of joint account all account holders have to submit the declaration PAN/Form 60 required for KYC updation.

FOR BRANCH USE Date of acknowledgement to customer

Verified in CBS on…… Signature Verified from CBS by ……(Sign of Official)

CUSTOMER ACKNOWLEDGEMENT COPY

A/c No/ID No:

Declaration and documents received for Re-KYC.

ACKNOWLEDGEMNT DATE …… SIGNATURE OF BANK OFFICIAL/SEAL

Annexure-23

(SELF DECLARATION IN CASE OF THERE IS CHANGE OF ADDRESS ONLY IN KYC INFORMATION INCLUDING PAN/Form 60 OF INDIVIDUAL CUSTOMER)

Name of Account Holder…….

Account/Customer ID Number……(Need not to submit separately for multiple accounts, ID is must in multiple accounts)

Contact/Mobile Number:……

I submit that there is no change in KYC information except change in my address details which is submitted hereunder:

MAILING ADDRESS

……

……

CITY…… PIN CODE……..STATE……..

I also undertake that I have already submitted PAN No…… /Form 60(whichever is not applicable to be strike off)

(Signature of accounts holders)

Enclosure: Valid Address Proof (Present Address)

In case of joint account all account holder has to submit the declaration PAN/Form 60 is required for KYC updation.

FOR BRANCH USE Date of acknowledgement to customer

Verified in CBS on…… Signature Verified from CBS by ……..…… (Sign of Official)

CUSTOMER ACKNOWLEDGEMENT COPY

A/c No/ID No:

Declaration and documents received for Re-KYC.

ACKNOWLEDGEMNT DATE ……SIGNATURE OF BANK OFFICIAL/SEAL

Annexure-24 (For Individuals)

Re-KYC / Periodic Updation Form
(Change in KYC and Other details)

Photo	Photo	Photo

ACCOUNT NUMBER (S)			
NAME			
Sr. No.	Parameter	Type	Number
1.	Identity Proof		
2.	Communication Address Proof		
3.	Permanent Address Proof		
PERSONAL DETAILS			
Father's Name			
PAN , if not available mention Form 60 Number			
City of Birth			
Nationality			
Marital Status		Married / Unmarried	
Wish to update contact details (Y/N)		If Yes, Mobile No: E Mail ID :	
Office/ Communication / Mailing Address			
Permanent Address			

Are you politically exposed	• I am a Politically Exposed Person. (Y / N) • Related to Politically Exposed Person(Y/N)
Occupation	
If Salaried, Employer Name	
If Self Employed, Type of employment	
If Business , Type of Business	
Nature of business	
Annual Income in case of salaried / Annual turnover in case of Business / Self-employed.	
Major Source of Fund	

Declaration: I hereby declare that the details furnished above are true & correct to the best of my knowledge & belief and affixing my signature in individual capacity. I hereby undertake to inform the bank of any changes therein immediately.

I hereby further declare and confirm that in the event any of the above information is found to be FALSE or UN-TRUE or MIS-REPRESENTING, the bank reserves the right to take necessary action including but not limited to freezing my account.

Date:

Place:

Signature / Thumb Impression of customer **FOR BRANCH USE Date of acknowledgement to customer** Verified in CBS on…… Signature Verified from CBS by ……
(Sign of Official)

CUSTOMER ACKNOWLEDGEMENT COPY

A/c No/ID No:

Declaration and documents received for Re-KYC.

ACKNOWLEDGEMNT DATE …… SIGNATURE OF BANK OFFICIAL/SEAL

Annexure-25

(SELF DECLARATION IN CASE OF NO CHANGE IN KYC INFORMATION OF LEGAL ENTITY CUSTOMER)

I undertake that there is no change in my KYC information as already submitted to the bank for

Name of Account ……

Account/Customer ID Number……

Contact/Mobile Number:……

REGISTERED ADDRESS OF LEGAL ENTITY ……

CITY…… PIN CODE……..STATE……..

COUNTRY……..

MODE OF OPERATION……AS PER DEED……RESOLUTION DEED

I /We also undertake on behalf of legal entity that PAN NO…… /Form 60(whichever is not applicable to be strike off) has already been submitted.

(……) (……) (……...) Signature of authorized signatory 1 Signature of authorized signatory 2 Signature of authorized signatory 3

*Mandatory field

#beneficial owner declaration to be provided in case beneficial owner information is not provided earlier. PAN is mandatory for company/partnership accounts.

FOR BRANCH USE Date of acknowledgement to customer

Verified in CBS on…… Signature Verified from CBS by ……
(Sign of Official)

CUSTOMER ACKNOWLEDGEMENT COPY

A/c No/ID No:

Declaration and documents received for Re-KYC.

ACKNOWLEDGEMNT DATE …… SIGNATURE OF BANK OFFICIAL/SEAL