

KYC Policy Guidelines

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and Section 9(14) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India, the Reserve Bank of India in exercise of the powers conferred by Sections 35A of the Banking Regulation Act (AACS) 1949, read with Section 56 of the Act *ibid*, issued directions for the regulated entities (REs) to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

The Bank is committed to implement KYC policy guidelines in letter and spirit while undertaking transactions on various deposit products offered by it and the terms & conditions governing the conduct of these products. . This policy is applicable to all customers of the Bank and outlines the principles for identification of all customers across the bank within the framework specified by the RBI as under:

- These Directions shall be called the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016.
- These directions shall come into effect from the date they are placed on the official website of RBI.

1. **Applicability:** The provisions of these directions shall apply to all the accounts maintained in all the branches of the Indraprastha Sehkari Bank Ltd.

2. **Definitions:** In these Directions, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:-

- i. "**Act**" and "**Rules**" means the Prevention of Money-Laundering Act, 2002 , the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 respectively and amendments thereto.
- ii. "**Aadhaar number**", as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.
- iii. "**Authentication**" means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
- iv. **Beneficial Owner (BO)**
 - a. Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

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

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

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

- d. Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- v. **Certified Copy of OVD**” - Obtaining a certified copy by bank shall mean comparing the copy of officially valid document 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 authorized officer of the Bank as per the provisions of the Act.
- vi. **"Central KYC Records Registry"** (CKYCR) means an entity defined under Rule 2(1)(aa) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- vii. **“Designated Director”** – The designated Director of the Bank shall be the Managing Director or a whole time Director duly authorized by the Board of Directors under Chapter –IV of PML Act and Rules.
- viii. **“Digital KYC”** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhar 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 authorized official of the bank as per provisions contained in the Act.

- ix. **“Digital Signatures”** shall have the same meaning as assigned to it in clause (p) of sub-section (1) of Section (2) of the Information Technology Act, 2000.
- x. **“Equivalent e-document”** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (preservation and retention of information by intermediaries Providing Digital Locker Facilities) Rules, 2016.
- xi. **“Know your Client (KYC) Identifier”** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- xii. **"Non-profit organizations"** (NPO) means any entity or organization that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 25 of the Companies Act, 1956.
- xiii. **“Officially Valid Document”** (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

- a) Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b) Where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-
 - i. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - ii. Property or Municipal tax receipt;
 - iii. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;
- c. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at ‘b’ above
- xiv. **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 under the Aadhaar regulations.

xv. **“Person”** has the same meaning assigned in the Act and includes:

- a. an individual,
- b. a Hindu undivided family,
- c. a company,
- d. a firm,
- e. an association of persons or a body of individuals, whether incorporated or not,
- f. every artificial juridical person, not falling within any one of the above persons (a to e), and
- g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xvi. **“Principal Officer”** means Chief Executive Officer/ an officer nominated by the Board of Directors, responsible for furnishing information as per rule 8 of the Rules.

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

xviii. **“Transaction”** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- a. opening of an account;
- b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- c. the use of a safety deposit box or any other form of safe deposit;
- d. entering into any fiduciary relationship;
- e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- f. establishing or creating a legal person or legal arrangement.

xix **“Suspicious transaction”** means a “transaction” as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:-

- a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b. appears to be made in circumstances of unusual or unjustified complexity; or
- c. appears to not have economic rationale or bona-fide purpose; or
- d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for

terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

- xx. **“Customer”** means a person who is engaged in a financial transaction or activity with the Branch and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- xxi. **“Walk-in Customer”** means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.
- xxii. **“Customer Due Diligence (CDD)”** means identifying and verifying the customer and the beneficial owner.
- xxiii. **“Customer identification”** means undertaking the process of CDD.
- xxiv. **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- xxv. **“Know Your Client (KYC) Identifier”** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- xxvi. **“Non-face-to-face customers”** means customers who open accounts without visiting the branch/offices of the Branch or meeting the officials of the branch.
- xxvii. **“On-going Due Diligence”** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers’ profile and source of funds.
- xxviii. **“Periodic Updation”** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
- xxix. **“Politically Exposed Persons”** (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
- xxx. **“Wire Transfer”** means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to beneficiary person at a bank;
- xxxi. **“Domestic and cross-border wire transfer”** when the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the ‘originator bank’ is located in different countries such a transaction is cross-border wire transfer.

3. Key Elements of KYC Policy

The KYC Policy has been framed to develop a strong mechanism for achieving the following objectives:-

- To prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities.
- Enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.
- To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms / AML standards / CFT measures / Bank's Obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.

The policy shall include the following four key elements:-

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

4. Money Laundering and Terrorist Financing Risk Assessment by REs:

(a) REs shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically 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, REs shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time.

(b) The risk assessment by the RE shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the RE. Further, the periodicity of risk assessment exercise shall be determined by the Board of the RE, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

(d) REs shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, REs shall monitor the implementation of the controls and enhance them if necessary.

5. Designated Director: The Board shall nominate a Director on the Board as —designated Director, as per provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

6. Principal Officer: The Principal Officer of the Bank, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law / regulations. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND. The Principal Officer will report to Designated Director

7. Compliance of KYC policy:

- a) The Branch Manager shall ensure compliance with KYC Policy through the senior officer /concerned officer for the purpose of KYC compliance.
- b) Allocation of responsibility through Office Order for effective implementation of policies and procedures at HO / Branches, including legal and regulatory requirements.
- c) Concurrent / internal audit system shall verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. Concurrent / internal audit to also ensure verification of compliance with KYC guidelines
- d) PML Rules require all offices of the Bank to carry out Risk Assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels. The risk assessment should-
 - (i) be documented;
 - (ii) consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
 - (iii) be kept up to date; and
 - (iv) be available to competent authorities and self-regulating bodies.

8. Customer Acceptance Policy: While opening any type of deposit account, the Branch shall ensure the following:-

- (i) No account is opened in anonymous or fictitious/ benami name(s);
- (ii) Documents and other information to be collected from different categories of customers depending on perceived risk and the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time.
- (iii) Not to open an account where the branch is unable to apply appropriate customer due diligence measures, i.e., the branch is unable to verify the identity and /or obtain required documents

either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

- (iv) The mandatory information required for KYC purpose is to be obtained from the customer while opening an account and during the periodic updation.
- v) The Branch shall apply the CDD procedure at the UCIC level(Customer ID). Thus, if an existing KYC compliant customer of a branch desires to open another. (account with the same branch, there shall be no need for a fresh CDD exercise.
- (vi) KYC documents are to be obtained for all the joint account holders, while opening a joint account.
- (vii) Circumstances in which, a customer is permitted to act on behalf of another person / entity, are clearly spelt out.
- (viii) The branch should 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.
- ix) Where Permanent Account Number (PAN) is obtained, the same shall be verified.
- x) Where an equivalent e-document is obtained from the customer, it shall be verified as per the provisions of the Information Technology Act, 2000.

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

9. Risk Management: All guidelines on implementation of KYC Norms issued by RBI from time to time will be implemented at all the branches. Customers shall be categorized as low, medium and high risk category based on the parameters such as customer's identify, social/financial status, nature of business activity, and information about customer's business and their location etc. While considering customer's identity, the Bank shall undertake confirmation of identity documents through online or other services offered by issuing authorities.

Risk categorization of the customer shall be on combination of the all the accounts in the Bank i.e. the customers' accounts should be linked to customer ID irrespective of constitution of account like Joint Account, Partnership Account etc.

On the basis of said risk profile, all the customers to be categorized as under:-

9.1 Low Risk Customers: Individuals (other than high net worth) and Entities whose source of wealth can be easily identified and transaction in whose accounts by and large confirms to their known sources of income and activities and small business enterprises whose annual turnover is not more than Rs.15.00 Lacs, etc.

The examples of low risk customers are as under:-

- (i) Salaried employees whose salary structures are well defined.
- (ii) People belonging to low economic strata of the society whose accounts show small balances and small business enterprises whose annual turnover is not more than Rs.15.00 Lacs, etc.
- (iii) Government Departments and Government owned companies, regulators and statutory bodies etc.
- (iv) Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment).
- (v) Customers with long term and active business relationship with the Bank (who are not coming under High / Medium Risk) In such cases only basic requirement of verifying the identity and location of the customer are to be met. Only usual precaution under this category of account are required except cash transactions of Rs.5.00 Lacs and above which are required to be monitored, recorded, and reported as per Rules. Annual turnover in such accounts should not exceed the known/declared source of income of the customer i.e. annual salary or business turnover etc., with a maximum variation of 10%.

9.2 Medium Risk Customers: Customers who are likely to pose a higher than average risk to the bank should be categorized as medium risk. For this category, higher due diligence is required which includes customers back ground, nature and location of activity, source of funds etc.

Firms and other individuals having annual turnover of Rs.300.00 Lacs or maximum balance of Rs.25.00 Lacs in their accounts are covered under this category. In addition to usual precaution, all cash transactions of Rs.5 Lakh and above and other transactions of Rs.25.00 Lacs and above are to be monitored.

The following customers are classified as medium risk customers:-

- (i) Stock brokerage
- (ii) Import / Export
- (iii) Car Dealer
- (iv) Electronics (wholesale)
- (v) Travel agency
- (vi) Used car sales
- (vii) Telemarketers
- (viii) Providers of telecommunications service, internet café, IDD call service, phone cards, phone center.
- (ix) Dot-com company or internet business.
- (x) Sole practitioners or Law Firms (small, little known) Accountants

- (small, little known firms)
- (xi) Professionals
 - (xii) Self-Employed
 - (xiii) Pardanashin

9.3 High Risk Customers: For this category higher due diligence is required which includes customers background, nature and location of activates, source of funds and his client profile etc.

All customers having annual turnover of more than Rs.300.00 Lacs or maintaining a balance of more than Rs.25.00 Lacs on an average (whichever is higher) in their accounts will fall in this category. Close monitoring of transactions in the account of customer under this category is required on day to day basis to ascertain that only genuine trade transactions are routed through their accounts. All transactions of Rs.25.00 Lacs and above are to be monitored, besides all cash transactions of Rs.5.00 Lacs and above.(Reporting as per rules).

The following customers are classified as high risk customers:-

- Trust, charities, NGOs and organization receiving donations. Accounts of cash intensive businesses such as accounts of jewelers and bullion dealers.
- Companies having close family shareholding or beneficial ownership.
- Firms with ‘sleeping partners‘.
- Politically Exposed Persons (PEPs).
- Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- Those with dubious reputation as per public information available.
- Accounts of non-face-to-face customers.
- High net worth individuals
- 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.
- 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.
- Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.
- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale.
- Customers that may appear to be Multi-level marketing companies etc.

9.4 All the branches are advised to categorize the customer/accounts under high risk category:-

- As and when complaints from legal enforcement authorities are received or fraud is reported against the customer and account holder.
- Blocked Accounts.
- Suspicious Transaction Report (STR) filed for the customer.

- Frequent cheque return in the account.

9.5 Roles and responsibilities of Branches:

- Branches shall review Customer risk categorization based on the risk categorization generated by the system, every six months./or as advised by the RBI from time to time.
- Branches may also apply additional alert indicators to address specific risks faced by them.

10. Customer Identification Procedure (CIP)

10.1 Customers Identification means: means identifying customers and verifying his/her identity by reliable/independent sources, documents, data or information, etc. Branch must obtain sufficient information necessary to establish to bank's satisfaction the identity of each new customer whether regular or occasional and also the purpose for which he/she intend to establish banking relation with our bank. The Branch shall observe the due diligence based on the risk profile of the customer in compliance with the extant guidelines in place.

10.2 Branch to undertake identification of customers in the following cases:

- a) Commencement of an account-based relationship with the customer.
- b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- c) Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
- d) When Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- e) Introduction is not to be sought while opening accounts.

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

- a) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
- b) Adequate steps are taken by Branch to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

- c) The third party is regulated, supervised or monitored for, and has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- d) The third party shall not be based in a country or jurisdiction assessed as high risk.
- e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Branch.
- f) 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.

11. Customer Due Diligence (CDD) Procedure

11.1 CDD Procedure in case of Individuals: For undertaking CDD, Branch shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

- a) A certified copy of OVD containing details of his identity and address.
- b) One recent photograph.
- c) The Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962.

Such other documents pertaining to the nature of business or financial status specified as under:-

- i. Atleast one document or the equivalent e-document thereof in support of the declared Profession / activity, nature of business or financial status, annual income, turnover (in case of business) such as salary slip, Registration certificate, Certificate / licence issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST / VAT / GST certificates, Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence / certificate of practice issued by any professional body incorporated under a statute, Complete Income Tax Returns (Not just the acknowledgement) etc.
- ii. However, customers who don't have business / financial activity or don't have any proof in this regard such as housewife, student, minor, labour working in unorganized sector, farmers etc may submit self-declaration to this effect.
- iii. Aadhaar from an individual if he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
- iv. The customer decides to submit his Aadhaar number voluntarily to the bank for identification purpose.

Provided that, where the customer has submitted, Aadhaar number under clause (ii) above, bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India upon receipt of the customers

declaration that he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of Aadhaar in his account.

Where the customer submits proof of possession of Aadhaar under (iii) above where the Branch may carry out offline verification.

***Explanation 1:** Bank shall, where its customer submits his proof of possession of Aadhaar Number containing 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.*

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

IMP: While establishing an account based relationship with individual customer, the branch official shall ascertain as to whether the customer is already having a Cust ID with the Bank. In case the customer has an existing Cust ID, fresh Cust ID shall not be created and the new account shall be opened with the existing Cust ID. The name, father's name, date of birth and address of the customer be filled in the same manner and style as it appears in the KYC document provided by the Customer.

The branch official will ensure that all the mandatory fields in Account Opening Form such as Name, Fathers' name , date of birth, address, Identity Proof, address proof, Identification number (Identity proof document number) , Profession / activity (Nature of Business - specific), total annual income, total annual turnover (in case of business) etc. are completely and correctly filled in by the customer and are also correctly captured in customer's database in CBS as risk category of the customer is assigned on the basis of these parameters.

In order to verify the authenticity of the KYC document, the authorized officer shall online verify Officially Valid Document (OVD) & PAN card details furnished by the customer from central authentic database, wherever available, in public domain. A print of on-line verification of the said document be held on record with the Account Opening Form.

In case an Individual customer who does not possess any of the OVDs and desires to open a Bank Account, Banks shall open a Small Account, which entails the following limitations:

- The aggregate of all credits in a financial year does not exceed rupees one lakh;
- The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

- The balance at any point of time does not exceed rupees fifty thousand.

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

- Further, small accounts are subject to the following conditions:
- The bank shall obtain a self-Attested photograph from the customer.
- The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

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

- Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
- Banks shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
- The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
- The entire relaxation provisions shall be reviewed after twenty four months.
- The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established through the production of OVDs and PAN or form 60 as the case may be.

11.2 Measures for Sole Proprietary Firms:

Customer shall be established through the production of an OVD and Permanent Account Number or Form No.60 as the case may be. For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

In addition to the above, any two of the following documents or the equivalent document thereof as a proof of business / activity in the name of the proprietary firm shall also be obtained:

- Registration certificate
- Certificate / Licence issued by the municipal authorities under Shop and Establishment Act.
- Sales and income tax returns.
- CST / VAT / GST certificate (provisional / final).
- Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
- IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- 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.
- Utility bills such as electricity, water, and landline telephone bills.
- 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. Provided Bank undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

11.3 CDD Measures for Legal Entities

11.3.1 For opening an account of a **company, certified copies of each of the following documents shall be obtained:-**

- Certificate of incorporation;
- Memorandum and Articles of Association;
- Permanent Account Number of the company;
- A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
- Documents, as specified for establishing the identity of an Individual, specified in Part-I shall be obtained relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

11.3.2 For opening an account of a **partnership firm, the certified copies of each of the following documents shall be obtained:-**

- Registration Certificate
- Partnership deed
- Permanent Account Number of the partnership firm
- Documents, as specified in Part-I, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

11.3.3 For opening an account of a **trust, certified copies of each of the following documents shall be obtained:-**

- Registration certificate
- Trust deed
- Permanent Account Number or Form No.60 of the trust; and

- Documents, as specified Part-I, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

11.3.4 For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents shall be obtained:

- Resolution of the managing body of such association or body of individuals
- Permanent account number or Form No.60 of the unincorporated association or a body of individuals;
- Power of attorney granted to transact on its behalf
- Documents, as specified in Part-I, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
- such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trusts / partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies.

11.3.5 For opening accounts of juridical persons, not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents shall be obtained:-

- Document showing name of the person authorized to act on behalf of the entity.
- Documents, as specified in Part-I, of the person holding an attorney to transact on its behalf.
- Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

11.3.6 For opening an account of Hindu Undivided Family, certified copies of each of the following documents shall be obtained:-

- Identification information as mentioned under Part-I in respect of the Karta and Major Coparceners,
- Declaration of HUF and its Karta,
- Recent Passport photographs duly self-attested by major co-parcen.

11.4 Identification of Beneficial Owner: For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps to be taken to verify his / her identity keeping in view the following :-

- (a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
- (b) In cases of trust / nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary is

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

12. On-going Due Diligence:

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

Monitoring of transactions is must. Following types of transactions shall necessarily be monitored:

- (a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- (b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
- (c) High account turnover inconsistent with the size of the balance maintained.
- (d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

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

- a. A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, or as specified by the RBI and the need for applying enhanced due diligence measures shall be put in place.
- b. The transactions in accounts of marketing firms, especially accounts of Multi- level Marketing (MLM) Companies shall be closely monitored.

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

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

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

13.1 Individual customers

13.1.1 No change in KYC information: In case of no change in KYC information, a self-declaration from the customer in this regard shall be obtained.

13.1.2 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 and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification etc. The Bank, at its option, may obtain a copy of OVD for the purpose of proof of address declared by the customer at the time of period updation. Such requirement, however, shall be clearly specified by the Bank in its Board approved KYC policy.

13.1.3 Minor Accounts: 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. Whenever required, the Bank 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.

13.2 Other than Individuals:

13.2.1 No change in KYC information: In case of no change in KYC information of the legal entity a self-declaration in this regard shall be obtained from such customer through its email id registered with the Bank. It shall further be ensured that Beneficial Owner information available them is accurate and shall keep it as up-to-date as possible.

13.2.2 Change in KYC information: In case of change in KYC information, the Bank shall undertake the KYC process equivalent to that applicable for on-boarding a new legal entity customer.

13.2.3 Additional measures, in addition to the above:

- a) Bank may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post etc. shall be acceptable.
- b) Bank shall ensure to provide acknowledgement with date of having performed KYC updation.
- c) In case of existing business relationship which is not KYC compliant or KYC has not been updated as per prescribed periodicity, Bank shall temporarily cease operations in the account. However, before temporarily ceasing operations for an account, the Bank shall give the client two notices of 10 days each and within 30 days period the account should be made KYC compliant otherwise operations in the account shall be frozen. The account holders shall have the option to revive their accounts by submitting KYC documents.

- d) The time limits prescribed above would apply from the date of opening of the account/last verification of KYC.
- e) In case of existing customers, Bank shall obtain the Permanent Account Number or the equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing with Bank shall temporarily cease operations in the account till the time the Permanent Account Number or the equivalent e-document thereof or Form-60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank shall give the client an accessible notice and a reasonable opportunity to be heard.

However, operations in accounts of customers who are unable to provide Permanent Account Number or the equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes, may allowed to be continued. The Branch Head shall allow such relaxation for continuation of operations in such accounts till the time PAN or the equivalent e-document thereof or Form 60 is obtained from the customer for which an officer from the branch will be deputed to personally visit the customer for obtaining the PAN or the equivalent e-document thereof or Form 60. However, the Branch Head shall ensure that such accounts are subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a Bank gives in writing to the Bank that he does not want to submit his Permanent Account Number or the equivalent e-document thereof or Form No.60, Bank 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.

14. Enhanced Due Diligence

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

14.2 Accounts of Politically Exposed Persons (PEPs): Bank shall have the option of establishing relationship with PEPs, provided that:

- Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
- The identity of the person shall have been verified before accepting the PEP as a customer;

- The decision to open an account for a PEP is taken at a senior level, i.e. at the level of Chief manager and above, in accordance with the Bank' Customer Acceptance Policy;
- All such accounts are subjected to enhanced monitoring on an on-going basis;
- In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval i.e. Chief Manager and above is obtained to continue the business relationship;
- The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

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

14.3 Client accounts opened by professional intermediaries: The Bank shall ensure while opening client accounts through professional intermediaries, that:

- a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- b) Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- c) Bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.
- d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Bank, and there are 'sub- accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Bank, the Bank shall look for the beneficial owners.
- e) Bank shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

The ultimate responsibility for knowing the customer lies with the Bank.

15. Simplified Due Diligence:

15.1 Simplified norms for Self Help Groups (SHGs)

- CDD of all the members of SHG shall not be required while opening savings bank account of SHG.
- CDD all the office bearers shall suffice.
- No separate CDD as per the CDD procedure mentioned in Section 15 of the members or office bearers shall be necessary at the time of credit linking of SHGs

16. Record Management: Following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. Bank shall,

- (a) Maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for at least five years from the date of transaction;
- (b) Preserve the records pertaining to identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
- (c) Make available the identification records and transaction data to the competent authorities upon request;
- (d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
- (e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following :
 - the nature of the transactions;
 - the amount of the transaction and the currency in which it was denominated;
 - the date on which the transaction was conducted; and
 - the parties to the transaction.
- (f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
- (g) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

17. Monitoring of transactions:

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

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

- The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND from time to time.
- While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Branch shall not put any restriction on operations in the accounts where an STR has been filed. Branch shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.
- Robust software throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

17.2 Reports to be furnished to Financial Intelligence Unit – India.

17.2.1 Cash Transaction Report (CTR):

- Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh. However, individual entries below Rs. 50,000/- will not be reported in the Cash Transaction Report.
- The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.
- A copy of monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch /HO for production to auditors/Inspectors, when asked for.

17.2.2 Suspicious Transaction Reports (STR): While determining suspicious transactions, the bank will be guided by the definition of suspicious transactions as contained in PMLA rules as amended from time to time.

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

- gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to not have economic rationale or bona-fide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

- It is likely that in some cases transactions are abandoned / aborted by customers on being asked to give some details or to provide documents. Bank will report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction.
- Bank to submit STRs if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
- Bank will ensure furnishing of STR within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.
- Bank will ensure not to put any restrictions on operations in the accounts where an STR has been filed. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.
- The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by the Head Office who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions.

17.2.3 Risk based transaction monitoring – customer behavior

- Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the institution to verify.
- Customer expressing unusual curiosity about secrecy of information involved in the transaction.
- Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
- Customer giving confusing details about a transaction.
- Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.

- Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
- Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.
- Customer's representatives avoiding contact with the branch.
- Customers who repay the problem loans unexpectedly.
- Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
- Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.
- Customer regularly issues large value cheques without balance and then deposits cash.
- Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

17.2.4 Transactions Involving Large Amounts of Cash

- Exchanging an unusually large amount of small denomination notes for those of - higher denomination;
- Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
- Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
- Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
- 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, e.g. cheques, letters of credit, bills of exchange etc.;

- 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.

17.2.5 Transactions that do not make Economic Sense

- A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
- Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

17.2.6 Activities not consistent with the Customer's Business

- Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
- Corporate accounts where deposits & 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.
- Unusual applications for DD/TT/PO against cash.
- Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
- Retail deposit of many cheques but rare withdrawals for daily operations.

17.2.7 Attempts to avoid Reporting/Record-keeping Requirements

- 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.
- Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
- 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.

17.2.8 Unusual Activities

- An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.
- A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
- Funds coming from the list of countries/centers, which are known for money laundering.

17.2.9 Customer who provides Insufficient or Suspicious Information

- A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
- A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
- A customer who has no record of past or present employment but makes frequent large transactions.

17.2.10 Certain Suspicious Funds Transfer Activities

- Sending or receiving frequent or large volumes of remittances to/from countries outside India.
- Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
- Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

17.2.11 Certain Bank Employees arousing Suspicion

- An employee whose lavish lifestyle cannot be supported by his or her salary.
- Negligence of employees/willful blindness is reported repeatedly.

17.2.12 Bank no longer knows the true identity: When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.

Some examples of suspicious activities/transactions to be monitored by the operating staff-

- Large Cash Transactions
- Multiple accounts under the same name frequently converting large amounts of currency from small to large denomination notes
- Placing funds in term Deposits and using them as security for more loans.
- Large deposits immediately followed by wire transfers.
- Sudden surge in activity level.
- Same funds being moved repeatedly among several accounts.
- Multiple deposits of money orders, Banker's cheques, drafts of third Parties
- Multiple deposits of Banker's cheques, demand drafts, cross/ bearer.
- Cheques of third parties into the account followed by immediate cash withdrawals.
- Transactions inconsistent with the purpose of the account.
- Maintaining a low or overdrawn balance with high activity.

Check list for preventing money-laundering activities:

- a) A customer maintains multiple accounts, transfer 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).
- b) 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 money.
- c) 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.
- d) 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.
- e) A customer experiences increased wire activity when previously there has been no regular wire activity. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- f) A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
- g) 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.

- h) Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- i) Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- j) Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
- k) Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- l) Periodic wire transfers from a person's account/s to Bank haven countries.
- m) A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- n) 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
- o) 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 lakhs), the amount is just under a specified threshold, the funds come from a foreign country or such transactions occur repeatedly.
- p) 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)
- q) A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

17.3.Counterfeit Currency Report (CCR): Cash transactions where forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security document has taken place facilitating the transactions, will be reported to Financial Intelligence Unit, India, in the specified format by 15th of the succeeding month.

17.4.Non Profit Organisations Transaction report [NTR] : Bank will report all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.

17.5. Requirements/obligations under International Agreements

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

- (a) The “**ISIL (Da’esh) & Al-Qaida Sanctions List**”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at <https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl>.
- (b) The “**1988 Sanctions List**”, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at <https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl>.

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

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.

17.5.2 Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967: The procedure laid down in the UAPA Order dated March 14, 2019 (Annex I of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

18. Other Instructions

18.1 Secrecy Obligations and Sharing of Information:

- a) Banks shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
- b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
- c) While considering the requests for data/information from Government and other agencies, banks shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

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

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

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

- a) Branches shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR.
- b) The KYC data / documents pertaining to all new individual accounts opened on or after January 1, 2017 have to be invariably uploaded with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

At each Branch, the Branch Manager /Accountant will be responsible for compliance of KYC Policy in the respective Branch.

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

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

22. Collection of Account Payee Cheques: Account payee cheques for any person other than the payee constituent shall not be collected.

- a) **A Unique Customer Identification Code (UCIC)** shall be allotted while entering into new relationships with individual customers as also the existing customers by bank.

- b) The bank shall not issue UCIC to all walk-in / occasional customers such as buyers of pre-paid instruments / purchasers of third party products. However, UCIC shall be allotted to such walk-in customers who have frequent transactions.

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

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

24. Debit Cards/Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc. Adequate attention shall be paid by the branches to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing aforesaid products/services/technologies.

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

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

- (a) The 'at par' cheque facility offered by commercial banks to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising therefrom.
- (b) The right to verify the records maintained by the customer cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements shall be retained by banks.
- (c) the Bank shall, therefore, ensure that the 'at par' cheque facility is utilised only:
- i. for their own use,
 - ii. for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,
 - iii. for walk-in customers against cash for less than rupees fifty thousand per individual.
 - iv. maintain the following:
 - v. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque,

- vi. sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.
- vii. ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved

27. Hiring of Employees and Employee training:

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